SWIFT EMAIL VERIFIER

SWIFT EMAIL VERIFIER USER MANUAL V3.0

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT US FOR A COPY.

IN NO EVENT SHALL ANONYPROZ LIMITED OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING,WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF ANONYPROZ LIMITED OR ITS AFFILIATTES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

SWIFT EMAIL VERIFIER: User Guide V3.0
Copyright © 2015 Anonyproz . All rights reserved.

Website: http://www.webemailverifier.com

Email:service@webemailverifier.com

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership
relationship between Anonyproz and any other company.

SWIFT EMAIL VERIFIER

Contents

EMAIL VERIFICATION TECHNOLOGY OVERVIEW 3
INTRODUCTION 4
ACCESSING SWIFT EMAIL VERIFIER 4
AVAILABILITY AND DASHBOARD INSTANCES 5
UPLOADING MAILING LISTS 5
IMPORTING EMAILS FROM MYSQL /SQL DATABASE 11
DELETING MAILING LISTS 14
EMAIL VALIDATION LEVELS AND CORRESPONDING SPEEDS 15
STARTING EMAIL VALIDATIONS AND RETRIEVING RESULTS/STATISTICS 16
CHECKING REMAINING VALIDATION QUOTA 20
VALIDATION STATUSES AND DETAILS 21
SAVING VALIDATION RESULTS AND CLEANING LISTS 25
USING YOUR CLEANED EMAILS IN THIRD PARTY EMAIL DELIVERY SERVICES 25
DELETING INVALID/UNKNOWN EMAILS DIRECTLY FROM A DATABASE 27
RE-VALIDATING UNKNOWN RESULTS 28
RECOMMENDED PRACTICES FOR DEALING WITH UNKNOWN RESULTS 30
GREYLISTING DETECTION AND HANDLING 30
DETECTING CATCH-ALL EMAIL DOMAINS & ROLE ACCOUNTS 31
ACTION STATUS 34
EMAIL VALIDATION BACKGROUND JOBS 34
VALIDATING REMAINING EMAILS IN STOPPED JOB 36
RESETTING VALIDATION JOBS 37
REMOVING RECORDS FROM THE GRID 38
BOUNCE HANDLER AND MAILING LIST CLEANING 39
HOW TO USE BOUNCE HANDLER AND MAILING LIST SUBTRACTION MODULE 45
DISCONNECTING FROM SWIFT EMAIL VERIFIER 49
FREQUENTLY ENCOUNTERED ISSUES AND TROUBLESHOOTER 49
FREQUENTLY ASKED QUESTIONS 50
GETTING SUPPORT 52

SWIFT EMAIL VERIFIER

EMAIL VERIFICATION TECHNOLOGY OVERVIEW

Email verification comprises a set of actions aimed at determining whether a specific email address is valid or not by simulating email sending. To understand how email verification works, it is necessary to understand first how sending of emails works. There are 2 stages in e-mail message delivery to the addressee:

1. The sender's mail server determines the addressee's mail server using DNS service;

2. The sender's mail server connects to the addressee's mail server via the SMTP protocol and transmits the message.

Hence to validate an email address, it's necessary to emulate these stages. Email verification works by connecting to the recipient's mail server, and imitates sending a message. When the server gives a response that the appropriate email address is good or bad, the email verifier disconnects from the server and marks the email address accordingly. No message is actually sent to the recipient. For a complete email validation, 2 stages of operations are normally performed.

During the first stage, the application uses DNS requests to check e-mail addresses availability. In this stage, it requests the DNS server for the mail server address of the mail domain. If the DNS server returns one or more addresses of mail servers which accept mail for the domain, the initial e-mail address is considered available and valid. If the address was not found by the DNS server at all or there are no mail servers which accept mail for the mail server, it is considered Invalid.

In the second stage of the email validation process, the email verifying software establishes connection to the mail server via the SMTP protocol (based on TCP). The TCP protocol is connection-oriented, so the servers dispatch service packages to establish the connection. After the connection is established, the servers exchange hello message. Then the sender's address is transmitted and the receiving server submits the message from this address to be accepted. Then the addressee's address is transmitted.

SWIFT EMAIL VERIFIER

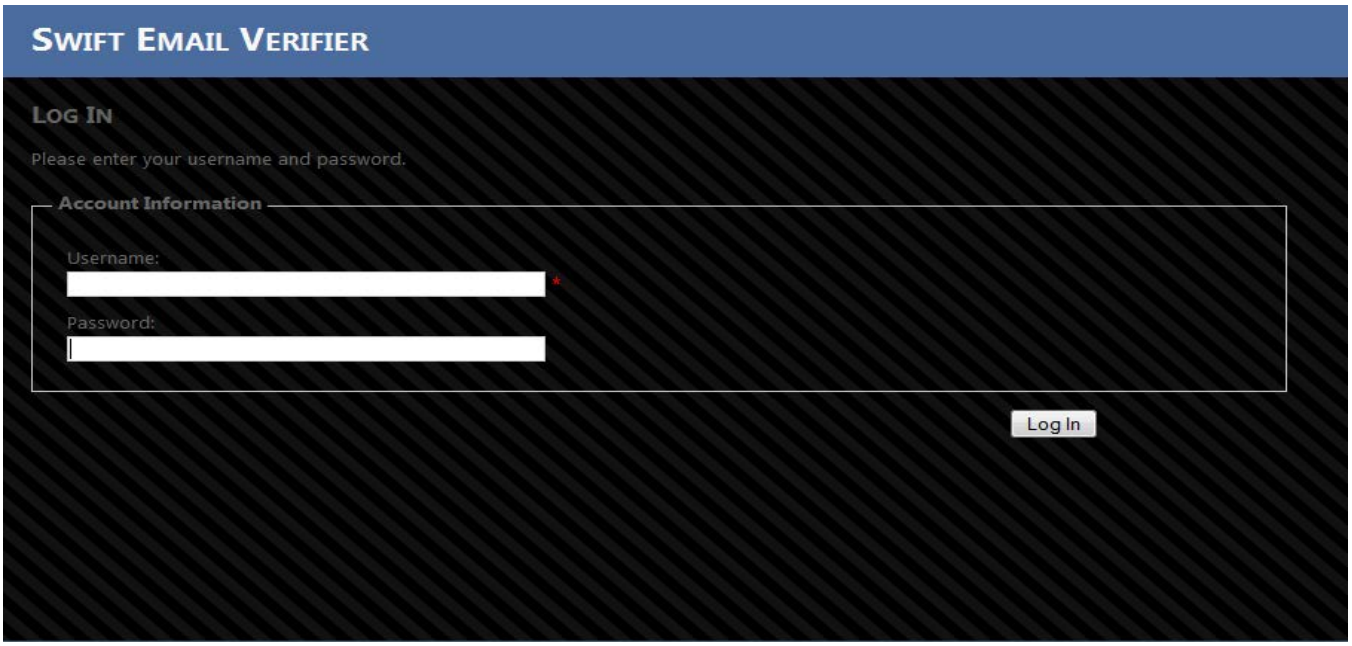
INTRODUCTION

Swift Email Verifier is a web based email verification service which enables you to verify your email lists and maintain a clean mailing list for your email marketing campaigns. In addition, you can use the in-built Bounce Handler module in Swift Email Verifier to process email addresses that could not be verified as Valid or Invalid while performing the email verification and ensure that your list is 100% clean.

Our powerful and fast web-based email verifier has the advantage that it can be used to verify your email lists in situations where you cannot use your regular desktop email verifier programs due to ISP SMTP port 25 blocking or lack of suitable client for your operating system. Our email verification service is completely web based and can be assessed using any browser. Click here to learn more on how Swift Email Verifier works.

ACCESSING SWIFT EMAIL VERIFIER

Swift Email Verifier is a web based software and as such you need a browser such as Firefox, Maxthon or Chrome to access the application. Once you have signed up and your account has been activated, you can login to the verifier URL using the login details that you have provided during your signup. The logon screen of the application looks like as it is shown in the screenshot below



AVAILABILITY AND DASHBOARD INSTANCES

In order to ensure continuous service availability in the event of unexpected downtime, we offer the possibility to access the verifier dashboard via a primary and secondary server. Both instances URLs will be provided in the welcome email you will receive when you signup. Validations can be started from any of the URL and the results can only be retrieved from the same instance from which the validation job was started.

Please note that when you have an active batch verification job running and you close the browser, you will be unable to access the page unless you close the whole browser and open the URL again due to session state. To address this, if you are running an active job in your account and you close the browser and you wish to access the application again, you can use the alternate URL. Both URLs can be alternated in the event of connection issues. Regardless of the URL used, your verification results data can be retrieved from any of the instances.

In addition, note that any mailing list you upload in a specific instance URL is only available locally in that dashboard instance. After loading the list and performing the validations, the results can only be retrieved from the same instance from which the validation job was started. Hence when you upload a file on a specific instance URL, this uploaded file will not appear on other instances. Any mailing lists uploaded are specific to each instance of the verifier dashboard.

UPLOADING MAILING LISTS

Swift Email Verifier supports only 2 types of mailing list formats. The mailing list can be uploaded in either TEXT or CSV (Comma Separated Values) formats. Note that Custom fields or extra information such as names, zip codes, addresses or phone numbers are supported and may be present in the mailing lists. If the mailing lists contain extra information, the validation results will also retain the extra information and will be available for download in the original format with all columns preserved.

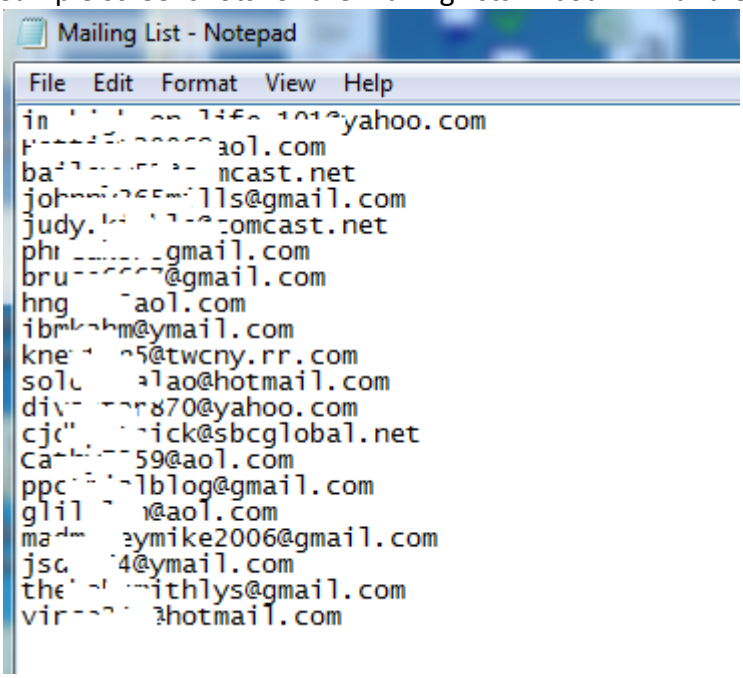
If your mailing list is in Excel format, please use a free Excel to CSV converter program to convert the Excel file to a CSV file before importing it into the verifier. You can download the program from this link.

To use the program take the steps below:

- Browse for input Excel file to convert.
- Browse for desired output folder & enter a file name.
- Click the CONVERT button.

The converted CSV file will be in the output folder specified.

Sample screenshots for the mailing lists in both TXT and CSV formats are shown below:



Mailing List in .txt format

	A	B
1	i _ ' ' ~n_life_101@yahoo.com	
2	Ho. ~~6@aol.com	
3	ba'' , ~@comcast.net	
4	joh. . ~~~ills@gmail.com	
5	j'' ', ' ' ~e@comcast.net	
6	p' ~3r@gmail.com	
7	br~~~~7@gmail.com	
8	h ~~~s@aol.com	
9	ib~ ~.m@ymail.com	
10	kr ' ~@twcny.rr.com	
11	sol~~~ ~lao@hotmail.com	
12	div~~' ~0@yahoo.com	
13	cjdk, ' ~@sbcglobal.net	
14	Cath, ~ ~@aol.com	
15	ppc~ ~g@gmail.com	
16	gli' ~@aol.com	
17	ma ' , ~e2006@gmail.com	
18	js. ~1@ymail.com	
19	the' ' ~hlys@gmail.com	
20	vir ~@hotmail.com	
21		

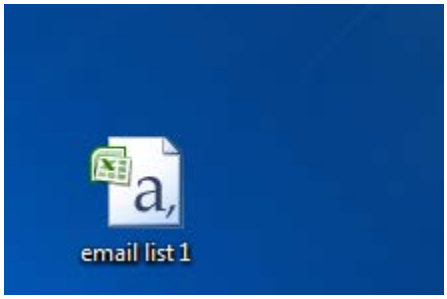
Mailing list in .csv format

SWIFT EMAIL VERIFIER

Ta	.@yahoo.com	2125 Gwene Ln	PORT ALSWORTH	AK	99653
Li	s@labor.state.ak	1111 W 8th St	Juneau	AK	99801-180
Ke Dist	k12.ak.us	148 N Binkley St	Soldotna	AK	99669-752
J E	@nycmail.com	12110 Business Blvd - Eagle	EAGLE RIVER	AK	99577
M	@graphics.com.com	2209AinakaheleSt.	ANCHORAGE	AK	99503
L Div	@state.ak.us	330 Willoughby Ave	Juneau	AK	99801-172
P ns	@audax.net	7645 King St # A	Anchorage	AK	99518-305
S ner	@sadiecove.com	2001 Seward Hwy	Seward	AK	99664 000
ub	@hotmail.com	PO Box 101504	ANCHORAGE	AK	99509
L ting	@hughesair.com	PO Box 770437	EAGLE RIVER	AK	99577
I	@akrdc.org	null	ANCHORAGE	AK	99501
Is s	@Island-Services	PO Box 214	Unalaska	AK	99685-021
Y or	@ykhc.org	4700 Business Park Blvd # E	Anchorage	AK	99503-712
D ior	@admin.state.ak.us	2301 Peger Rd	Fairbanks	AK	99709-539
N	@nnorthwind-inc.cc	235 E 8th Ave # 210	Anchorage	AK	99501-365
A	@alaskapacificbank.con	2094 Jordan Ave;	Juneau	AK	99801
L	@kidsarepeople.org	851 Westpoint Dr # 104	Wasilla	AK	99654-718
L y	@northstar.k12.ak.	601 F St	Fairbanks	AK	99701-380
V	@awt.alaska.net	401 East Northern Lights Bl	ANCHORAGE	AK	99503
ra	@lithia.com	4700 Gambell St	Anchorage	AK	99503-743
S mer	@ptialaska.net	2001 Seward Hwy	Seward	AK	99664 000
M nc	@matanuska.com	163 E Industrial Way	Palmer	AK	99645-670
D	@gci.net	1310 W. 32nd Ave	ANCHORAGE	AK	99503

Mailing list in .csv format with extra information

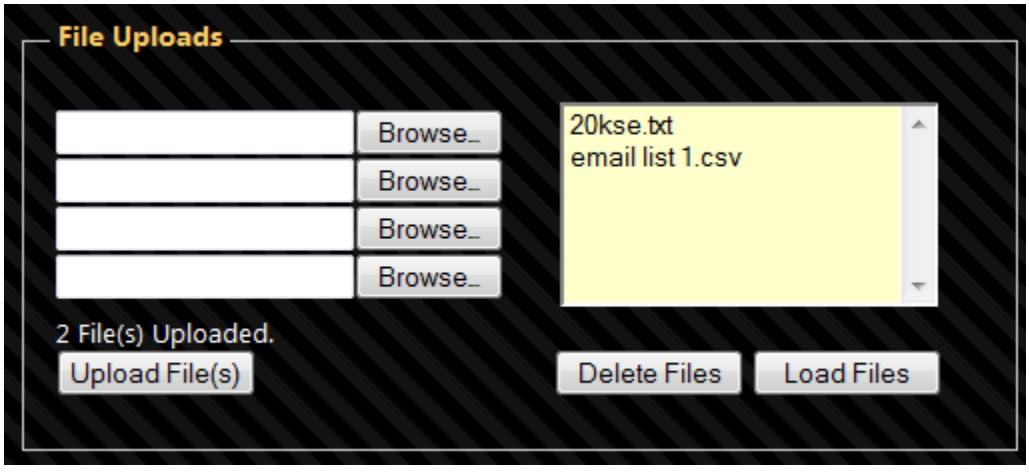
Please do not confuse Excel files with CSV files. You can easily identify a Microsoft Office CSV file by the file icon with "**a,**" which should look like the one shown in the screenshot below:



Note: Please make sure all emails have no spaces as any email with spaces will have the sign "?" when loaded into the verifier which will invalidate the emails. A sample is illustrated below:

Email	Email Local Part	Email Domain	Email TLD	Status	Details
k@lyndworld.com		lyndworld.com	com		
r@newhome1.com		newhome1.com	com		
taint@newhome1.com		newhome1.com	com		
@associatedestates.com		associatedestates.com	com		
jis.com		sares-regis.com	com		
@laramarapts.com		laramarapts.com	com		
@newhome1.com		newhome1.com	com		
@lyndworld.com		lyndworld.com	com		
lyndworld.com		lyndworld.com	com		
@qwestoffice.net		qwestoffice.net	net		
legacypartners.com		legacypartners.com	com		
@newhome1.com		newhome1.com	com		
@lyndworld.com		lyndworld.com	com		
@597westport-apts.com		597westport-apts.com	com		
bridgesatmallardcreek-apts.com		bridgesatmallardcreek-apts.com	com		

To upload the mailings list, simply click on the “Browse” button in the verifier interface and browse to the location where the mailing list is located on your computer. You can upload up to 4 mailing lists at the same time as shown below. Once you have located all the mailing lists, click on “Upload Files” button to begin the upload process. Depending on the size of your mailing lists, this upload process can take a while. Please note that in order to ensure system stability and prevent system resources abuse, you are allowed a maximum of 20MB batch size of mailing lists for each validation job. This is to ensure that all users have available resources to use. However, you can run as many batches as you want while your subscription is active.



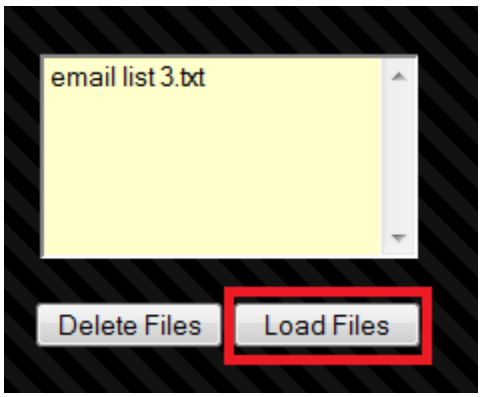
The screenshot below shows the action indicator while the list is being uploaded. Please be patient while the file upload process is in progress.

Once the upload process has finished, you will see the uploaded mailing lists in the box as shown above. In addition, the email addresses contained in the mailing list(s) will be analyzed and displayed in the Grid table as shown below:

Email	Email Local Part	Email Domain	Email TLD	Status	Details
		yahoo.com	com		
		yahoo.com	com		
		yahoo.com	com		
		yahoo.com	com		
		yahoo.com	com		
		yahoo.com	com		
		yahoo.com	com		
		yahoo.com	com		
		yahoo.com	com		
		yahoo.com	com		
		yahoo.com	com		
		yahoo.com	com		
		yahoo.com	com		
		yahoo.com	com		
		yahoo.com	com		
		yahoo.com	com		
		yahoo.com	com		
		yahoo.com	com		

This table will show the results of the email validations during the validations.

Any mailing list uploaded can be reloaded whenever needed. To reload the list, simply click on the “Load Files” button to load the mailing lists in the grid.



IMPORTING EMAILS FROM MYSQL /SQL DATABASE

Swift Email Verifier supports directly importing your email lists from your MySQL or SQL Server without the need of exporting the emails first. This gives you the flexibility to connect to your external MySQL or SQL Server powered database and import your emails with a few clicks. Importing email lists from an external MySQL or SQL database also allows you to preserve all other fields associated with your emails such as names, locations, zip codes, phone numbers etc.

For example, if you have a database of email addresses which includes extra information like names, physical address, phone no,etc. and you have this database in a MySQL or SQL database, you can use our verifier to connect directly to the MySQL or SQL database table which is holding only the email addresses and import the emails to the verifier interface and then proceed to validate them. After validating the emails, our verifier also will allow you to delete the invalid emails from the email table in the database directly.

However, please note that when the emails are deleted from the database table, only the table row containing the email will be deleted. All other data associated with the emails such as names, address, phone number etc will not be deleted. This is useful in case you wish to preserve your customer or subscriber data while making efforts to update the subscriber information with the correct email address.

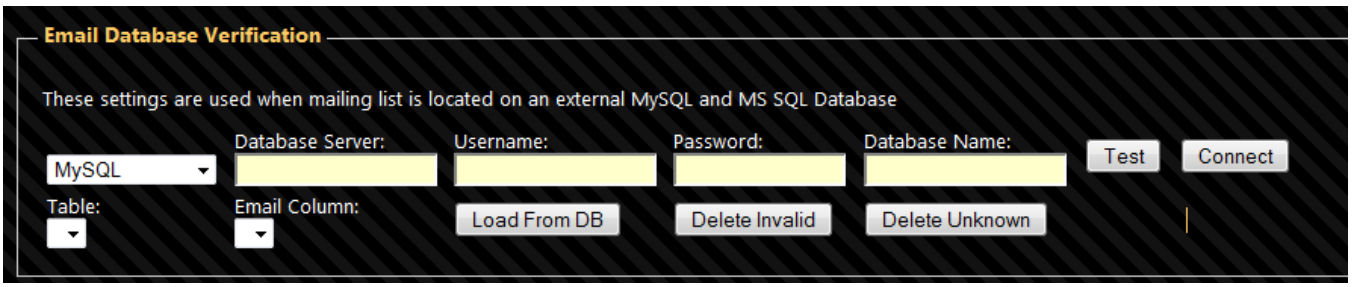
Important Security Information: When you connect to your database through our online verifier and import your emails, we DO NOT store any of your database connection information or credentials. Your database connection credentials is used in real-time to connect to your database securely through our SSL/HTTPS protected online verifier interface thereby making it impossible for any entity to sniff your database credentials in transit. These credentials are NEVER stored on the server.

To ensure that the credentials are transmitted securely over SSL, you must ensure that the web verifier URL is accessed using https. For example: https://URL-of–web-verifier. In addition, it is strongly recommended to restrict access to your database to speficic IPs or change your database password frequently for added security. If you wish to grant access to our verifier IP to connect to your database, please contact us and we will provide you the IPs.

Disclaimer: According to our TOS/AUP we are not responsible for unauthorized access to or alteration of your data sent through our servers.

To start importing emails from your external database, simply provide your database connection details and connect to the database. Once connected, the powerful wizard will automatically display the database tables and columns for the database. Once the column containing the emails is selected, the emails are then imported and populated in the verifier Grid system. The following illustrate the steps:

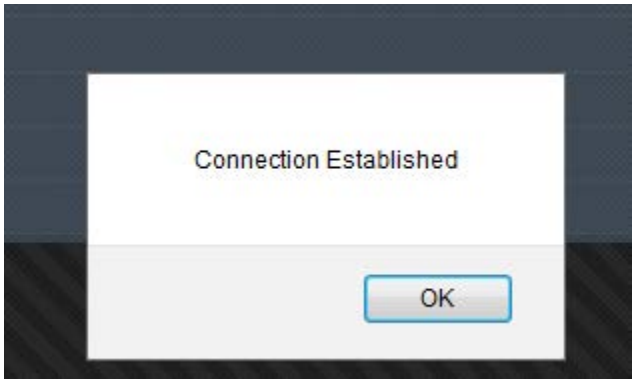
Step 1: Go to the "**Email Database Verification**" group in the verifier interface as shown below:



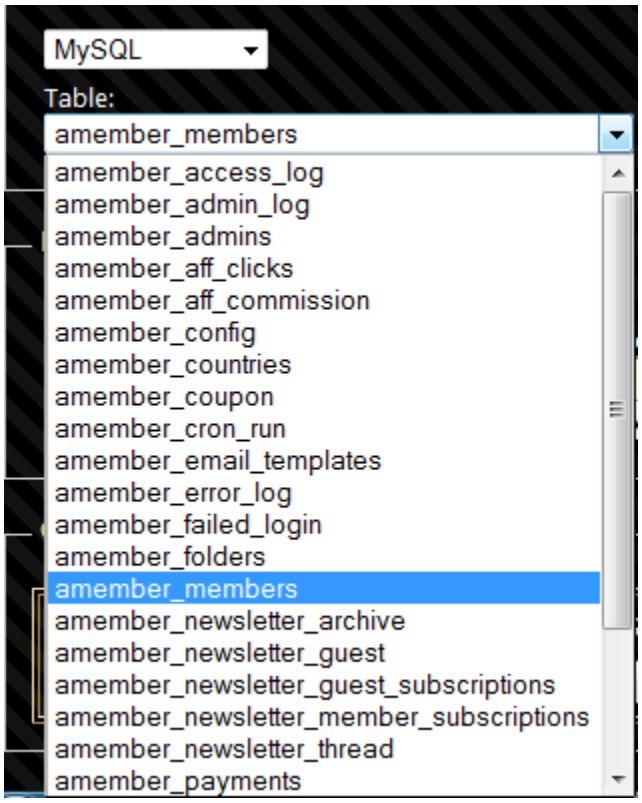
Step 2: Select the database type (MySQL or SQL Server) from the dropdown, and enter the Database server hostname/IP, Database name, Username and Password to connect to the database. These parameters are explained below:

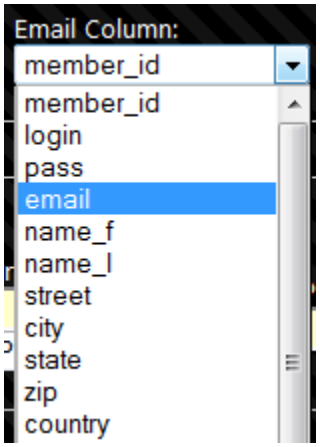
- **Database Server:** Enter the IP Address /Hostname of the database server
- **Database Name:** Enter the database name containing the mailing list
- **Username:** Specify the username to login to the database
- **Password:** Specify the password for the username

Step 3: Test the database connection by clicking on the "Test" button. Once a connection can be established, a pop-up window pops up showing "Connection Established" message appears. Click OK to proceed.



Step 4: Connect to the database by clicking on the "Connect" button. After a connection is successfully established, all the tables available in the database will be available in the "Table" dropdown box as shown in the sample screenshot below. Select the appropriate table containing the email lists to import. Then select the appropriate column in the selected table containing the email lists.





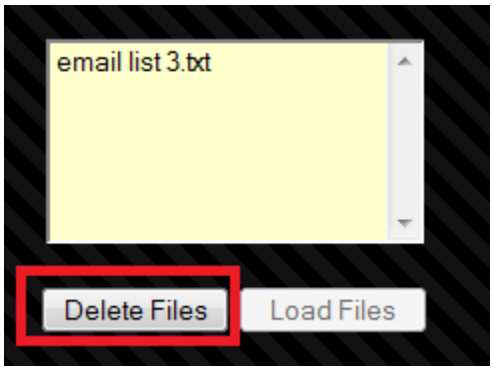
Step 5: Click on the "Load From DB" button to import the emails and load the emails on the verifier grid for verification. As soon as the emails are loaded, these will be visible in the grid.

Step 6: At this point the emails are now ready to be verified. To learn how to proceed to verify the emails, please skip to the "EMAIL VALIDATIONS AND RESULTS/STATISTICS" section.

The instructions dealing with how to delete invalid/unknown emails detected by the verifier directly from the database is explained on a separate section of this manual here.

DELETING MAILING LISTS

After performing the validations and when the results and the grid table have been saved, you may delete the lists by clicking on the "Delete Files" button. Once the mailing files are deleted, they are permanently deleted from the server and cannot be retrieved. The email records will also be deleted from the Grid system.



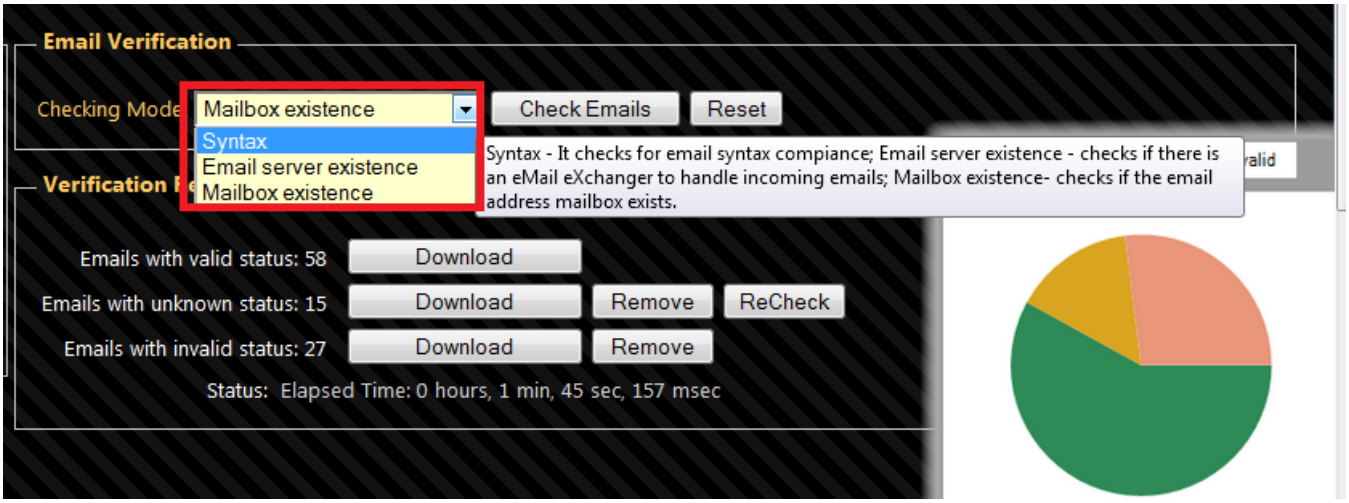
EMAIL VALIDATION LEVELS AND CORRESPONDING SPEEDS

Swift Email Verifier can perform 3 levels of validations as follows:

1. Syntax: This checks the email addresses and ensures that they conforms to IETF standards using a complete syntactical email validation engine

2. Email Server Existence: This level checks the availability of the email address domain using DNS MX records

3. Mailbox Existence: This is a deep level verification which attempts to check if the email address really exists and goes a step further to check if the email domain is a Catch-all domain (a domain that will receive all of the email messages addressed to that domain, even if their addresses do not exist in the mail server). The Mailbox verification establishes SMTP dialogs with external SMTP servers and this level usually requires longer time depending on multiple network factors.


Email Verification
Checking Mode
Mailbox existence
Check Emails
Reset
Syntax
Email server existence
Mailbox existence
Syntax - It checks for email syntax compiance; Email server existence - checks if there is an eMail eXchanger to handle incoming emails; Mailbox existence- checks if the email address mailbox exists.
Verification
Emails with valid status: 58
Download
Emails with unknown status: 15
Download
Remove
ReCheck
Emails with invalid status: 27
Download
Remove
Status: Elapsed Time: 0 hours, 1 min, 45 sec, 157 msec

You can select any one of these levels while performing your email validations. The Syntax and Email Server Existence levels of validations are very fast compared to the Mailbox existence level. With Syntax's being the lowest level and Mailbox Existence being the highest one

As the level increases, so generally does the time needed to perform the email validation; Syntax validation is typically instantaneous, while Mail Server Existence validations verifications may take some seconds to complete, depending on multiple network factors. The level to choose depends on your specific needs such as accuracy and speed.

Note: We do not recommend the use of the Syntax or Mail Server Existence check levels with your credits as this amounts to wastage of your validation quota unless you really need the Syntax or Mail Server Existence levels. Instead use the full email validation (Mailbox existence check) which includes also the Syntax and Mail server Existence checks. The checks are done in a progressive order and the highest order is the mailbox existence.

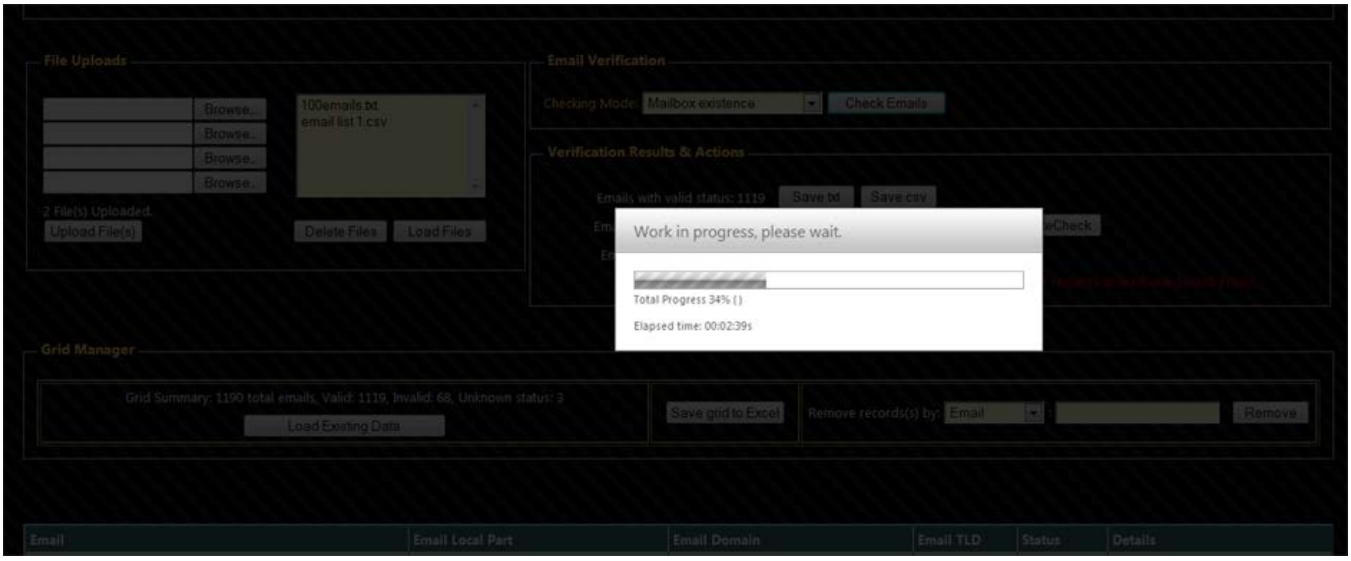
The table below provides a speed benchmark test we performed with the application for the three levels.

Level	No. of Emails	Time of Completion
Syntax	1,000	173 ms
Mail Domain Existence	1,000	50 seconds
Mailbox Existence	1,000	7 minutes

Note: Our email verifier can verify hundreds of emails per minute typically between 100-300 emails per minute when performing full email existence validations. This speed is the dedicated speed per user and not the overall simultaneous speed server-wide for all users using the verifier at any point in time.

STARTING EMAIL VALIDATIONS AND RETRIEVING RESULTS/STATISTICS

After selecting the right validation level, the validations is started by clicking on the “Check Emails” button. As soon as the validation is started, a progress bar pops up which shows you the progress of the validation job as shown in the screenshot below:



Once the progress bar reaches 100%, the validation job completes and the results is then displayed in the Grid and the software provides you with 3 results with 3 different colour codings as follows:

1. Valid

2. Invalid

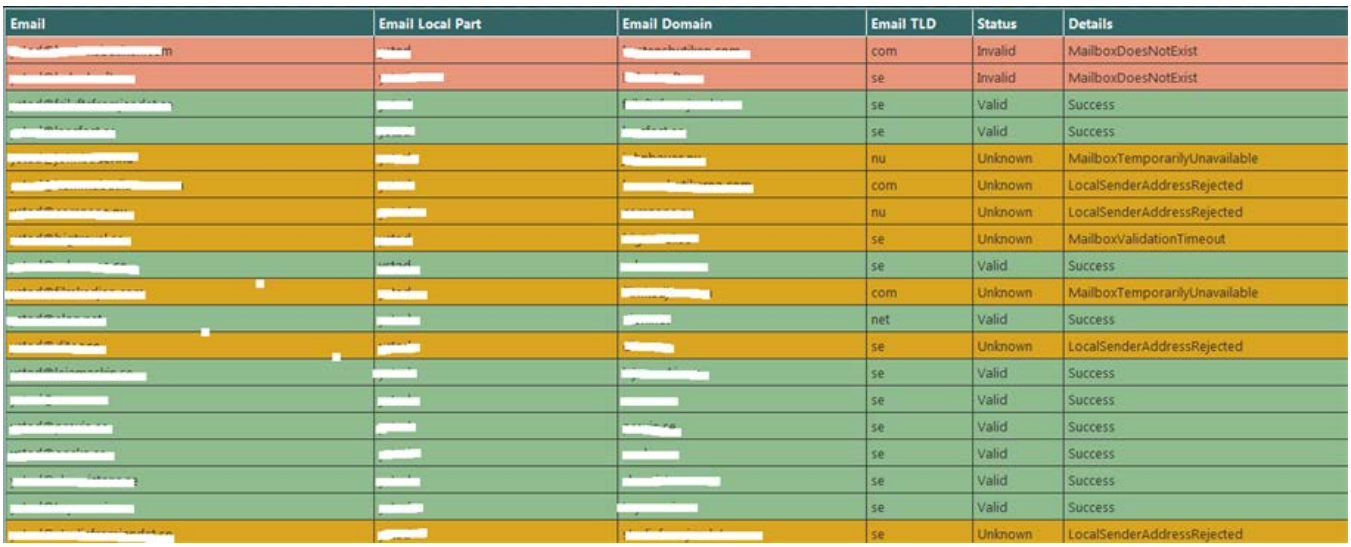
3. Unknown

In addition, after the validation job is completed, you will automatically be notified by email. A message will be sent to your email address on your account.

Note: After a validation job has completed, the verifier still needs some additional minutes to complete all processes running in the background. Hence, you may be unable to start a new validation job immediately after a recent validation job. Please always wait for at least 30 minutes in-between validation jobs before starting a new validation. If you wish to forcefully kill all background processes immediately after a validation job, you may use the “Reset” button.

This is how you will know if a running validation job has completed:

When you login to the verifier after some time of running your validation job, click on the "Load Existing Data" button and check the statistics of the results. If the result shows that it is equal to the total emails you have loaded originally for the job, then the job is complete. Then simply save the results. However, if the results statistics do not tally with the number of emails originally loaded, then it simply means that the job is still running in the background process of the verifier. In that case, just logout and login again after some more hours and check again using the "Load Existing Data" button until the job completes.



Email	Email Local Part	Email Domain	Email TLD	Status	Details
			com	Invalid	MailboxDoesNotExist
			se	Invalid	MailboxDoesNotExist
			se	Valid	Success
			se	Valid	Success
			nu	Unknown	MailboxTemporarilyUnavailable
			com	Unknown	LocalSenderAddressRejected
			nu	Unknown	LocalSenderAddressRejected
			se	Unknown	MailboxValidationTimeout
			se	Valid	Success
			com	Unknown	MailboxTemporarilyUnavailable
			net	Valid	Success
			se	Unknown	LocalSenderAddressRejected
			se	Valid	Success
			se	Valid	Success
			se	Valid	Success
			se	Valid	Success
			se	Valid	Success
			se	Valid	Success
			se	Unknown	LocalSenderAddressRejected

Please note that as soon as the active validation job has completed, it will show 100% in the progress bar but the verifier still needs few minutes to complete all processes. Please be patient. If the validation progress reaches 100% and doesn't stop after 30 minutes, then something might be wrong. In that case, you must do the following:

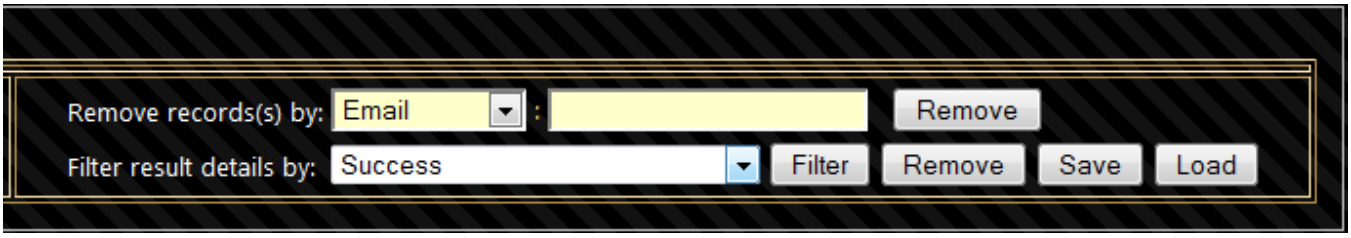
1. Log out from the verifier and login again. Then click on the "Load Existing Data" button to retrieve the results.

2. Examine the results statistics and confirm if the total emails you have loaded were validated. If this is so, then your job has completed. Simply save the results and you are done.

3. If the results do not display the full emails loaded for the validation job, then something must have gone wrong. Due to the nature of the verifier application environment, it is normal for the job to stop during the verification process due to server timeout or downtime issues. To fix this, you must kill the job by clicking on the "Reset" button and wait for about 3-5 minutes for this action to propagate in the server. Then click on the "Load Existing Data" button to retrieve the already completed job results and make sure you save the results to your computer. Then finally reload the remaining emails that have not been verified by clicking on the "Load Remaining Emails" button. After you load the list, run the verification on these remaining emails which were not verified before the job stopped.

Important: Please note that clicking the “Load Remaining Emails” button will delete the current or last completed validation job results already completed in the system. Therefore, you must ensure that you have saved the results before performing this action.

The Grid system displays the table of the validation results which shows the status of each email address. The result statuses for each email address will also be displayed in the grid for investigating the reason of a specific email validation failure. These validation statuses can be filtered easily using the filter button as shown below and the results can be removed, saved (CSV format) or re-loaded into the grid for a new validation job as desired using the appropriate buttons.



Note: Whether you choose to accept the email addresses returned for each status code depends on your use case, and may require case-by-case manual evaluation.

Please be aware that you can take advantage of the integrated automated bounce handler feature of the verifier to process bounced emails for those emails which could not be validated (unknown) due to

multiple reasons such as Graylisting, SMTP connection timeout, non-cooperating SMTP servers, expired/deactivated/suspended emails. Please note that most email servers will return VALID status for expired/deactivated/suspended emails. Hence, messages sent to these emails will bounce because they are not active.

In some cases, unknown results can also result from the inability to verify the emails by simulating a message sending to the recipient email server because the recipient email server requires that a REAL message is sent. Thus, it is impossible to verify whether the address is good or not. You won't know definitively until the message bounce because these mail servers won't cooperate or cannot be checked without sending a real message to them.

In addition, please be aware that some emails which returns unknown results could be valid. Examples of such emails which are flagged unknown by the verifier and which may be valid are:

• Disposable Email Addresses from email address providers, like Mailinator, 10MinuteMail, GuerrillaMail,etc

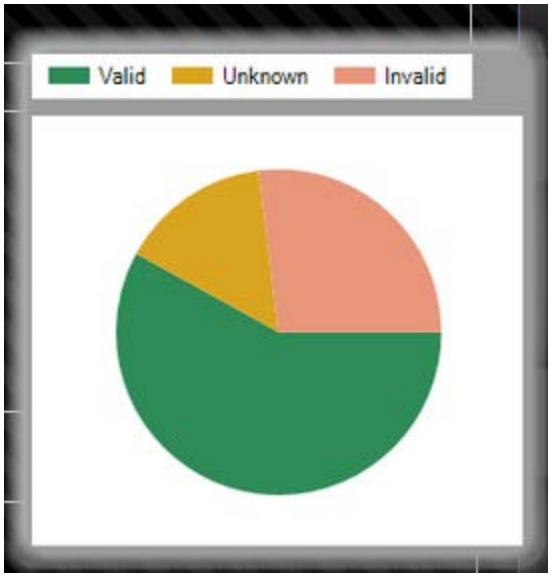
• Catch-all email addresses

• Temporarily Unavailable emails (Graylisting)

• Soft bounces

To take care of the unknown emails, download the unknown results and send your campaigns to the list and then use the in-built bounce handler in our verifier to process the bounces and download the bounce emails. Then after getting the bounce list, subtract it from the unknown results list. For details on how the automated bounce handling works, please click here.

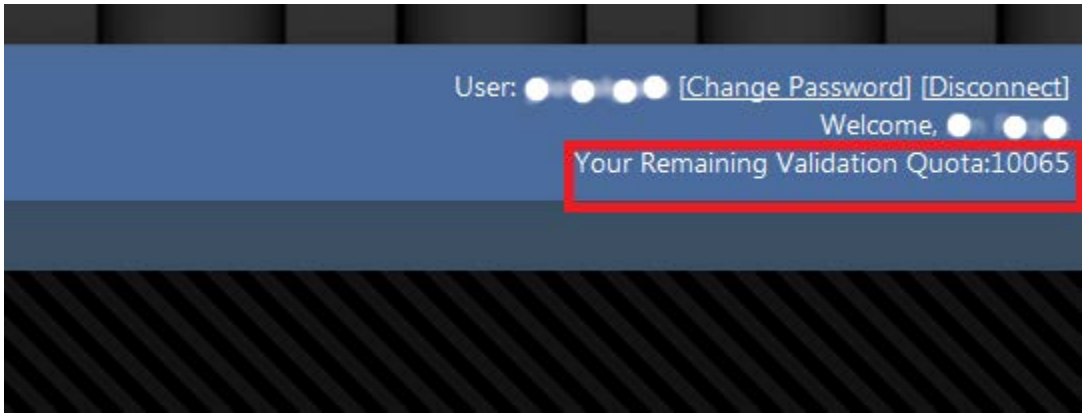
The results are also virtualized in a form of Pie Chart as shown below.



Important: All unknown email validation results from our email validation server will not count towards your email validation quota. This means that we will not charge credits from your quota when the result of a validation is unknown. Therefore you do not need to contact us anymore to replace the quota for the unknown results.

CHECKING REMAINING VALIDATION QUOTA

On the top right hand corner of your online dashboard account, you will see your remaining quota clearly displayed. Please always check it before you start any validation job and ensure that the number of emails you have loaded for the validation job is less than your current remaining quota.



Note: If you have exhausted your quota and you have an active validation job running, the validation job cannot proceed and you will be prompted with an error message. Hence, you must check your current quota limit before you start your validation. Make sure the number of emails loaded is less

than your current quota before starting the validation. If you wish to add additional credits or quota to your account, simply place an order for any additional credits on our website and the credits will be added to your existing quota automatically.

VALIDATION STATUSES AND DETAILS

Swift email verifier uses a specific "status" and "details" code to indicate the success or failure of the validation of an email address. The "Status" indicates the actual result of the validation (Valid, Invalid or Unknown) while the "Details" provides further information to indicate the success or failure of the email validation including specific details why the email validation has failed.

Swift Email Verifier defines the validity of an email address as follows using only 3 statuses:

Status	Description/Meaning
Valid	Mailbox exists and not handled by Catch-all domains or known to be a DEA
Invalid	Mailbox does not exists
Unknown	Mailbox could not be verified or is determined to be handled by a Catch-all domain, DEA, Greylisted,, SMTP/Mailbox timeouts, Temporary mailbox unavailability. Specific reason for failure is provided in the status codes.

Each of these Statuses is linked to the following Details:

Details	Meaning
Success	The email was successfully verified as Valid
InvalidCharacterInSequence	This failure means that an invalid character has been detected in the provided email address, like in the following example: `me@ex@mple.com`
InvalidWordBoundaryStart	This failure means that a new word boundary start has been detected at an invalid position, like in the following example: `hi.\\there@example.com`
UnmatchedQuotedPair	This failure means that a quoted pair within a quoted word in the provided email address is not closed properly.

UnexpectedQuotedPairSequence	This failure means that an unexpected quoted pair sequence has been found within a quoted word in the provided email address, like in the following example: `"find it in \§ 3"@example.com`
UnbalancedCommentParenthesis	This failure means that the number of parenthesis used to open comments in the provided email address is not equal to the one used to close them.
DoubleDotSequence	This failure means that an invalid sequence of two adjacent dots has been found in the provided email address, like in the following example: `where.is..it@example.com`
InvalidLocalPartLength	This failure means that the local part of the email address has an invalid length, according to the IETF standards.
InvalidFoldingWhiteSpaceSequence	This failure means that an invalid folding white space (FWS) sequence has been found.
AtSignNotFound	This failure means that the at sign symbol (@), used to separate the local part from the domain part of the address, has not been found, like in the following example: `me-at-example.com`
InvalidEmptyQuotedWord	This failure means that an invalid quoted word with no content has been found, like in the
	following example: `freddy."".krueger@example.com`
InvalidAddressLength	This failure means that the provided email address has an invalid total length.

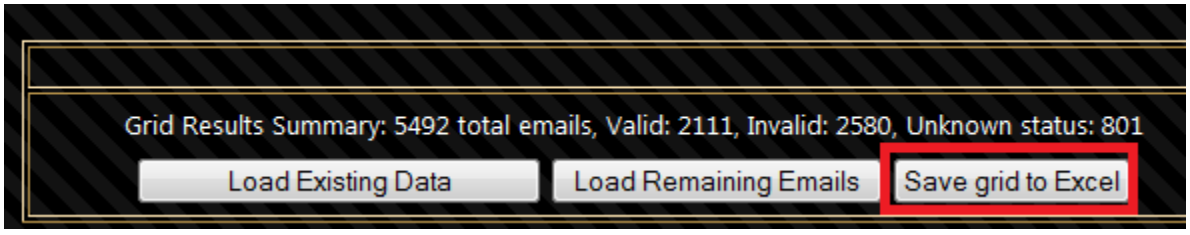
DomainPartCompliancyFailure	This failure means that the domain part of the email address is not compliant with the IETF standards, like in the following example: `michael@example."hi there".com`
DnsQueryTimeout	This failure means that a timeout has occurred while querying the DNS server(s) for records about the email address domain.
DnsConnectionFailure	This failure means that the verification failed because of a socket connection error occurred while querying the DNS server.
DomainIsInexistent	This failure means that the domain of the email address does not exist, like in the following example (at the time of this writing): alice@i-do-not-exist.xyz
DisposableEmailAddress	This failure means that the email address is provided by a well-known disposable email address provider (DEA) such as mailinator.com
SmtpConnectionTimeout	This failure means that a timeout has occurred while connecting to the mail exchanger which serves the domain for the provided email address.
SmtpConnectionFailure	This failure means that a socket connection error occured while connecting to the mail exchanger which serves the domain for the provided email address.
MailboxDoesNotExist	This failure means that the mailbox for the provided email address does not exist.
MailboxConnectionFailure	This failure means that a connection error occurred while validating the mailbox for the
	email address.
UnhandledException	This failure means that the external mail exchanger refused the SMTP connection.

LocalSenderAddressRejected	This failure means that the external mail exchanger rejected the local sender address or the incoming connecting IP.
MailboxValidationTimeout	This failure means that a timeout occurred while verifying the existence of the mailbox for the provided email address.
MailboxTemporarilyUnavailable	This failure means that the requested mailbox is temporarily unavailable; this is not an indicator that the mailbox actually exists or not but, often, a message sent by external mail exchangers with greylisting enabled.
ServerDoesNotSupportInternationalMailboxes	This failure means that the external mail exchanger does not support international mailbox names, while the provided email address uses a non-ASCII encoding for its local part.
ServerIsCatchAll	This failure means that the external mail exchanger under test accepts fake, non existent, email addresses; therefore the provided email address MAY be inexistent too. In most cases, these Catch-all domains are now setup by ISPs and ESPs as Catch-all Spam Trap domains specifically targeted to catch spammers using Dictionary Spam Attacks.
CatchAllValidationTimeout	This failure means that a timeout occurred while verifying fake email address rejection for the mail server. Note that emails which returns this status are marked Valid because it already passed the mailbox existence test.
CatchAllConnectionFailure	This failure means that a connection error occurred while verifying the external mail exchanger rejects inexistent email addresses. . Note that emails which returns this status are marked Valid because it already passed the mailbox existence test.

InvalidToken	An invalid API key was used. Please check the API key and make sure it is correct
NoMoreQueries	The allocated # of queries or requests for the API key has been exhausted.
InternalError	There was an unexpected error on our server.

SAVING VALIDATION RESULTS AND CLEANING LISTS

After the validation job is completed, the results can be saved either in text or CSV formats. To save the results, simply click on the "Save txt" or "Save csv" buttons for the result groups as desired. To delete the Unknown emails or the Invalid emails from the original mailing list, click on the "Remove" button beside each group. In addition, the full validation results from the Grid or table of results can be saved in Excel format for your records. To save the table of results or grid, click on the "Save Grid to Excel" button as shown below:


Grid Results Summary: 5492 total emails, Valid: 2111, Invalid: 2580, Unknown status: 801
Load Existing Data
Load Remaining Emails
Save grid to Excel

USING YOUR CLEANED EMAILS IN THIRD PARTY EMAIL DELIVERY SERVICES

Many companies and email marketers are now using third party email delivery services to handle the delivery of their transactional and marketing emails. By using a professional third party email delivery service, a higher inbox placement or delivery rate can be achieved. These third party email delivery services have relationships with various ISPs/ESPs and also provide strict acceptable "Bounce Rate" threshold for those who use their service to avoid being labeled as a server that delivers spam.

Although, the benefits of using a third party email delivery service is obvious, extreme care must be taken in order not to exceed the acceptable or permitted "Bounce Rate" for any email campaign you send through their platforms. Bounce rate is simply the percentage of emails that is returned undelivered when you send out your campaign. Although most third party email services do not

explicitly specify their bounce rate limit, as a rule of thumb, anything between 10-15% may be considered high.

The Bounce Rate is expressed as a percentage and is calculated as follows:

$$Bounce\_Rate = \frac{No.\_of\_Bounces}{Total\_No.\_Emails\_Sent} x100$$

Undeliverable emails, email "bouncebacks" or "bounces" are becoming more and more of a challenge for email marketers these days. Hence, all third party email delivery services has a specific allowed or permitted bounce rate for every email campaign you send using their services. If you exceed this rate, your account may be suspended or deactivated. In most cases, these third party email delivery services are required by ISPs/ESP and Spam Advisory Groups such as Spamhaus to enforce the bounce rate thresholds and suspend any account that exceeds these thresholds in order to prevent Spam.

In order to avoid your third party email delivery service account suspension or deactivation, it is important that you review and adopt the following best practices before importing your cleaned emails into your third party email delivery service as follows:

1. After validating your list, save the VALID emails marked by the verifier. Do NOT add the emails marked as Unknown to the valid emails. As a rule, never upload the unknown emails to your third party email delivery service.
2. After saving the VALID emails, download our “Role/One-way communication” emails suppression list from this link and use the List Suppression feature of our verifier to delete all matching role accounts and one-way communication emails from the valid email list that you have downloaded from the verifier. Role/one-way communications emails include such emails as service@domain.com, support@domain.com , donotreply@domain.com etc.

   Note that it is very important to delete role accounts/one-way communication emails from your list before importing them into your third email delivery service because the presence of such emails in your list is normally regarded as an indication that your list may be purchased or scraped. Hence, if you upload such list containing such emails, the list will be flagged and your account may be suspended.
3. Some email addresses marked as Valid by the verifier may not be Valid in reality. This false positive is caused by a strict anti-spam technology employed by some ISPs notably Yahoo. With Yahoo in particular, deactivated/suspended/expired emails are marked as Valid by the verifier because Yahoo regards these emails as valid or “existent” even though such emails are not active and

cannot receive emails. Hence when you attempt to send your campaigns to such emails, they will bounce because the emails are not active.

Thus, before using the valid emails downloaded from the verifier, it is strongly advisable to remove all Yahoo emails from the list. You can save the yahoo emails to a separate file and add them to the unknown emails and use the bounce handling feature of the verifier to process the bounces to such emails using a private bounce-to email address of your mail server. For details, please click here.

4. As we indicated above, never upload the emails marked as unknown by the verifier to your third party email delivery service provider platform. You must process all potential bounces to the unknown emails using a private mail server with the help of a bounce handler or a dedicated bounce handling service. Our verifier includes an automatic bounce handler. Using the bounce handler, you can then extract these emails and delete them from the unknown list before importing the list into your third party email delivery service.

   Approximately 24-72 hrs, the bounce handler can be used to connect to the bounce-to email address which will enable it login to the email account, read all bounced emails and extract the emails and collect them in a text file. You can then download the file and subtract them from the unknown list you downloaded from the verifier. In addition, if you have alternate contact information such as postal address or phone number for the subscribers whose emails has bounced, call or mail them a postcard to let them know their email bounced and you'd like to get an updated one. Also, it is recommended to offer your subscribers a way to update their email address and other account details somewhere on your website.

   To learn more about how the bounce handler works, please click here

DELETING INVALID/UNKNOWN EMAILS DIRECTLY FROM A DATABASE

Swift Email Verifier supports the import of emails directly from a MySQL or SQL Server and also the removal of the invalid or unknown emails directly from the database. Once the emails have been imported and verified, the invalid or unknown emails can be deleted directly from the database in order to clean the database from any invalid emails with a single click. After running the verification of the emails, both invalid and unknown emails can be removed from the database using the appropriate buttons on the Email Database Verification group in the verifier interface as shown below.

The following recommended practices are strongly recommended when performing database based email verification with Swift Email Verifier:

1. After performing the email validation, ensure that you save all the results locally to your computer and make a backup. The results can be saved in both TXT, CSV and Excel formats.

2. Delete all the invalid emails directly from the database by clicking on the “Delete Invalid” button. Please note that this action will directly connect to the database and delete the invalid emails. This operation cannot be reversed.

3. Using the validation results filter, carefully review the various unknown results status codes and use your discretion to determine which emails can be removed or considered more likely valid. Since some of the unknown results may indicate temporary issues, it may be helpful to re-validate the unknown results again or validate the emails using the bounce handler. Please click here to skip to the section which deals with this.

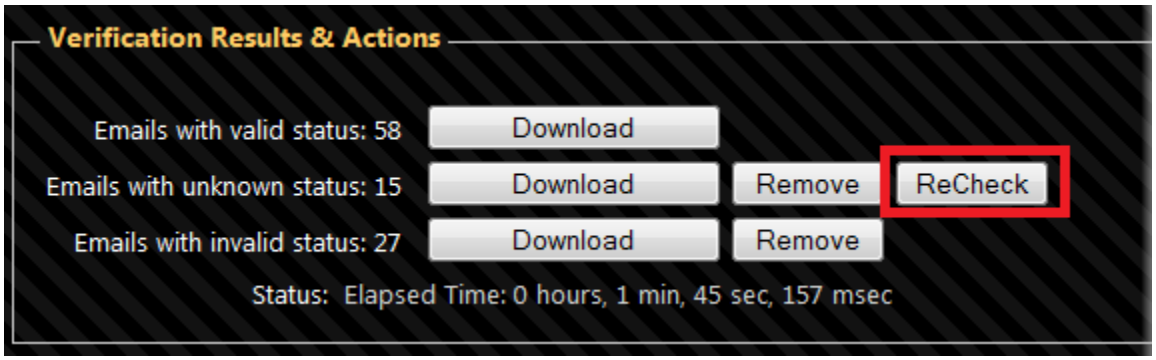
RE-VALIDATING UNKNOWN RESULTS

The Unknown results are those emails which could not be verified due to one reason or the other. These unknown results in most cases results from Greylisting which is technology that reduces spam by rejecting initial email delivery attempts. The Greylisting works by returning a "Temporarily Unavailable" message to the sending mail server the first (and only the first) time a message is received from a given sender. Hence, it makes sense to retry these validations again after some time has elapsed.

Also unknown results can also result from the inability to verify the emails by simulating a message sending to the recipient email server because the recipient email server requires that a REAL message is sent. Thus, it is impossible to verify whether the address is good or not. You won't know definitively until the message bounce because these mail servers won't cooperate or cannot be checked without sending a real message to them.

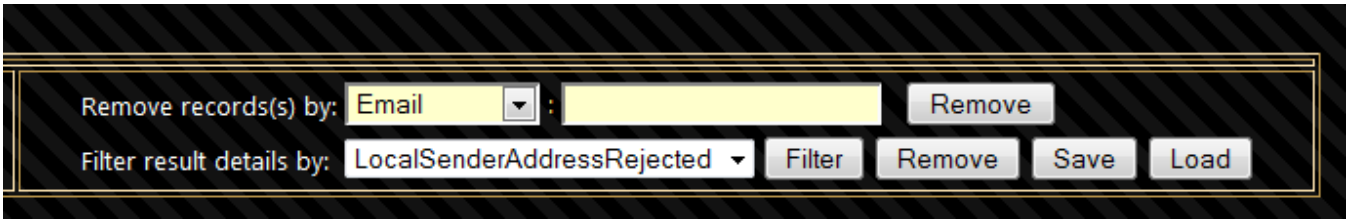
To accommodate for this, Swift Email Verifier includes an in-built bounce handling module that can be used to process the bounced emails to the unknown results list. Simply download the unknown results mailing list and send your campaign to the list using a bounce-to email address. Thereafter, use the bounce handling module to connect to the bounce-to email address and process the bounced emails which will then be subtracted from the unknown mailing list. You can run the Bounce Handler to process bounced emails during 2-5 days after you send your email campaign because bounced emails may arrive within 2-5 days. To learn more about how our bounce handling module works and how to use it, please skip to this page.

In addition, Swift Email Verifier includes a feature to enable you re-validate the unknown results again by clicking on the “Re-Check” button. When this button is clicked, the verifier automatically re-validates the emails with the Unknown status in the table of results and after completing the validations, automatically updates the table of results or Grid.



Note: Please note that if you did save the unknown results as a file after a verification job completes and wish to re-run it again at a later time, you must load this unknown list again and verify it normally but not by clicking the 'Recheck" button.

However, you do not have to save the unknown list first before re-validating it. You can re-check the full unknown emails immediately after running the mailing list verification by clicking on the 'ReCheck" button under the "Verification Results & Actions" group. If you wish to re-check specific unknown results status emails such as those related to timeout or temporarily unavailability, you must save these group statuses individually first by using the “filter” and “save” buttons in the Grid Manager before reloading them individually for rechecking by using “Load” button as shown below:



RECOMMENDED PRACTICES FOR DEALING WITH UNKNOWN RESULTS

The following recommended practices are strongly recommended to deal with the unknown results reported by the application:

1. Since a majority of the unknown results are caused by temporary issues (Soft Bounces) such as SMTP server timeout or downtime, Greylisting, Mailbox size Exceeds quota, temporary mailbox suspension/deactivation, and temporary blockings due to IP reputation, it is strongly recommend to re-validate the entire unknown list again at a later time. We do not recommend deleting the unknown list immediately after running your verification job. Chances are that previous emails which previously tested as unknown could test valid after re-validating the list.

2. Review all the failure status codes for the unknown emails. You can filter these statuses by using the filter button. Doing this will allow you to know why each email address in the unknown list could not be verified as valid or invalid. You may use your discretion to delete only those emails belonging to a status code which are more likely to indicate invalid emails and leave the rest. Please note that any emails deleted are permanently removed from the overall results .This action cannot be reversed.

3. After pruning the unknown list as explained above, you may then proceed to download the unknown list. This pruned unknown list can be later used for your email campaigns. We strongly recommend the use of the bounce handler module of the application to process any emails that may bounce and have these removed from the list. For details, on how this works, please click here.

4. If you have alternate contact information such as postal address or phone number for the subscribers whose emails has bounced, call or mail them a postcard to let them know their email bounced and you'd like to get an updated one. Also, it is recommended to offer your subscribers a way to update their email address and other account details somewhere on your website.

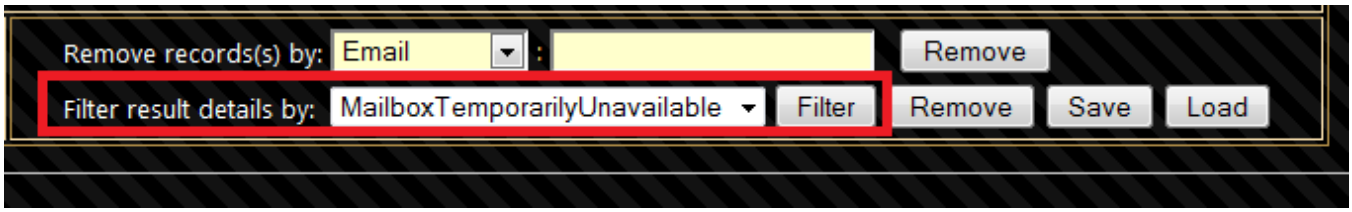
GREYLISTING DETECTION AND HANDLING

Swift Email Verifier comes with a powerful Greylisting detection and handling otherwise known as temporary mailbox handling which is technology that reduces spam by rejecting initial email delivery attempts. Greylisting works by returning a temporary failure response ("Temporarily Unavailable") to the first attempt to deliver an email, but accepts it on the second attempt. Thus every proper email server will attempt to redeliver a message after a temporary failure response.

While performing validations with Swift Email Verifier, any SMTP status code that reports a temporary unavailability of a mailbox will return the "**MailboxTemporarilyUnavailable**" verification status which indicates that the mail server has Greyisting enabled. To take care of this, the specific emails that returned this status code (MailboxTemporarilyUnavailable) can be filtered and re-loaded for re-validation after some time has elapsed.

The following steps show how Greylisting can be handled:

1. After running the validation, proceed to the "Grid Manager" group and go the "Filter results by" part and select "MailboxTemporarilyUnavailable" code from the dropdown box and click on the Filter button as shown below:



2. Click on the "Load" button to re-load the emails into the grid system. Please note that re-loading the emails will delete all current records on the grid.
3. Proceed to the "Email Verification" group and choose the "Mailbox Existence" level and click on "Check Emails" to re-validate the emails again
4. Wait for the verification to complete and save any emails that is re-checked as valid. You may repeat this process multiple times after some time until the desired results is obtained

DETECTING CATCH-ALL EMAIL DOMAINS & ROLE ACCOUNTS

Swift Email Verifier has the capability to automatically detect Catch-all emails which is a mailbox on an email domain that will receive all of the email messages addressed to that domain, even if their addresses do not exist in the mail server. This Catch-All domain test is performed at the "Mailbox Existence" level. First the checker engine checks if the mailbox being verified actually exists on the mail server and if this succeeds, it goes a step further to check if the email domain will receive all of the email messages addressed to that domain, even if their addresses do not exist in the mail server.

Thus emails that return "ServerisCatchAll" status may be VALID or INVALID. The emails could not be conclusively determined as VALID because the email server under test accepts fake, non-existent, email addresses; therefore the tested email address MAY be inexistent too. Therefore, it is impossible

to verify conclusively whether the email address is good or not. You won't know definitively until the message bounce.

Hence, to accommodate for this, Swift Email Verifier includes an in-built bounce handling module that can be used to process the bounced emails to the unknown results list. Simply download the unknown results mailing list and send your campaign to the list using a bounce-to email address. Thereafter, use the bounce handling module to connect to the bounce-to email address and process the bounced emails which will then be subtracted from the unknown mailing list. You can run the Bounce Handler to process bounced emails during 2-5 days after you send your email campaign because bounced emails may arrive within 2-5 days.

To learn more about how our bounce handling module works and how to use it, please click here.

In some cases, these Catch-all domains are now setup by ISPs and ESPs as Catch-all Spam Trap domains specifically targeted to catch spammers using Dictionary Spam Attacks. Most email servers do not have a Catch-all domain by default because the vast majority of emails that goes into a catchall email account are spam. Spam traps are emails that either don't exist, or exist solely for the purpose of catching unsolicited email. For a more detailed definition of a 'spam trap', look here: http://en.wikipedia.org/wiki/Spamtrap.

As more and more ISPs, ESPs and Anti-Spam organizations now operate Spam Traps in order to combat spam, it is important to get informed about Spam Traps and how to stay off from them. Please be informed that we do not detect Spam Traps with our email verifier service. Note that hitting a Spam Trap can affect your Sender Score and Reputation which is closely monitored by ISPs and ESPs such as Google, Yahoo, Hotmail etc. If you continually hit Spam Traps, your IP could be blacklisted. There are two types of spam traps employed by ISPs and Anti-Spam services and these are **Pure Spam traps** and **Recycled Spam traps.**

Pure Spam Traps are created for the sole purpose of being a spam trap. These Spam Traps are usually posted on websites, sometimes even hidden in the background code. In addition, majority are also setup as "Catch-all domains" in order to capture spammers using dictionary SPAM attacks. These Pure Spam Traps are normally picked up by email harvesting bots. If you are using our service legally and using the service to verify your opt-in email lists, you should not hit Pure Spam Traps. Using our service for verifying harvested or generated email lists is strictly against our TOS/AUP.

The second class of Spam Traps (Recycled Spam Traps) also known as dead addresses, dormant addresses, inactive addresses etc. are email addresses that were once owned by customers of the ISP/ESP that have stopped using the accounts. These types of addresses frequently trap legitimate senders with weak list hygiene and data quality practices. Many ISPs/ESPs will after a pre-defined but undisclosed period of email inactivity turn the account off and return hard bounce or SMTP errors to

senders. At some point, the ISP will reactivate (recycle) the address, convert it to a spam trap and allow email to be received by the email address. If a sender is sending to an address that has been deactivated and later reactivated, it can be indicative of poor mailing list hygiene and maintenance.

It is important to note that there's no magic radar detector for Spam Traps. In order to function properly and catch spammers, Spam Traps are designed to remain undetected. Therefore, the best course for avoiding spam traps is not detection, but prevention.

Finally, another class of damaging emails which must be removed from your mailing lists is known as Role Accounts or Function Email Accounts. A Role or Functional account is an email address that is not associated with a specific person, but rather with an office, position, and group such as: webmaster@domain.com, hostmaster@domain.com, sales@domain.com, support@domain.com, postmaster@domain.com, abuse@domain.com etc. Role-account addresses are usually posted on public Web pages which make them vulnerable to harvesters or bots and such emails normally end up in purchased lists. .

In addition, some blacklists deliberately use role addresses as "honeypots" to trap spammers and blacklist spammers IPs since any email sent to the addresses is regarded as spam by default since the address was obtained and used without permission.

The following best practices can be used to prevent and remove potential spam traps which an email marketer has acquired due to poor list hygiene and management.

Recommended Best Practices:

1. Do not harvest or generate email lists
2. Only purchase or rent mailing list from reputable data brokers. Purchasing mailing list from unscrupulous data brokers is not advisable because it could be loaded with harvested email addresses, including role accounts. If you rent or borrow a mailing list, have all role accounts suppressed before you send your campaigns to the emails. You can download our role accounts suppression list here. You are free to modify and add your own custom entries to the list.
3. Use a confirmed or double opt-in process to validate newly acquired email addresses before adding them to your lists
4. Use a bounce handler to promptly delete bounced emails from your mailing lists
5. Place unsubscribe links in your email campaigns and make sure the emails are deleted from your lists
6. Establish an on-going process for actively removing old and/or inactive subscribers

Detecting and Removing Role Accounts and One-Way Communication Emails with Swift Email Verifier:

1. Use the "Remove Records" feature to search and delete all "one-way communication "and "role/function" emails such as no-reply@domain.com, do-not-reply@domain.com,

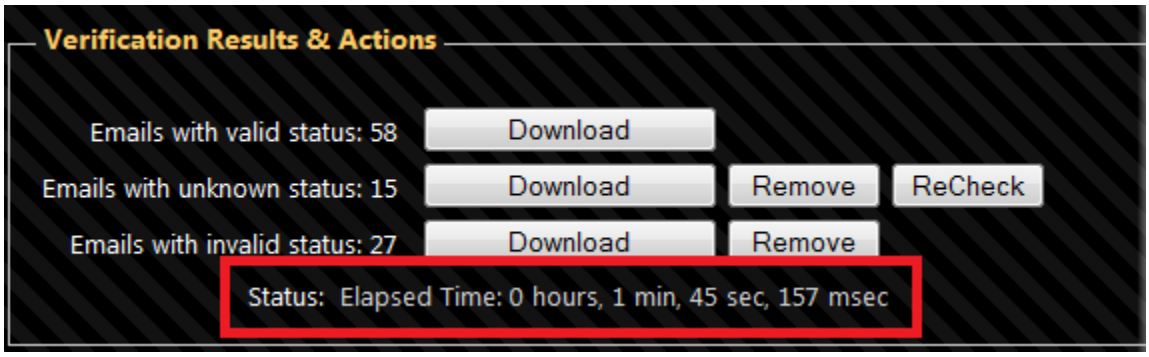
donotreply@domain.com, noreply@domain.com, webmaster@domain.com, hostmaster@domain.com, sales@domain.com, support@domain.com, postmaster@domain.com, abuse@domain.com etc.

2. Use the "Filter Result Details by" feature to filter and remove all email tests that returns "**ServerIsCatchAll**" as verification status. These emails could be potential Spam Traps

Note: Please be aware that we do not offer Spam Trap detection feature with our email verifier services. You should focus preventing hitting Spam Traps instead of detecting them.

ACTION STATUS

While using Swift Email Verifier, the status of any action performed with the application will always be displayed in the Status indicator depending on the actions being carried out as shown below. If you encounter any error or issues while running the application, these will also be displayed here also. If you need to contact us to report an issue, please take note of the status and report same.

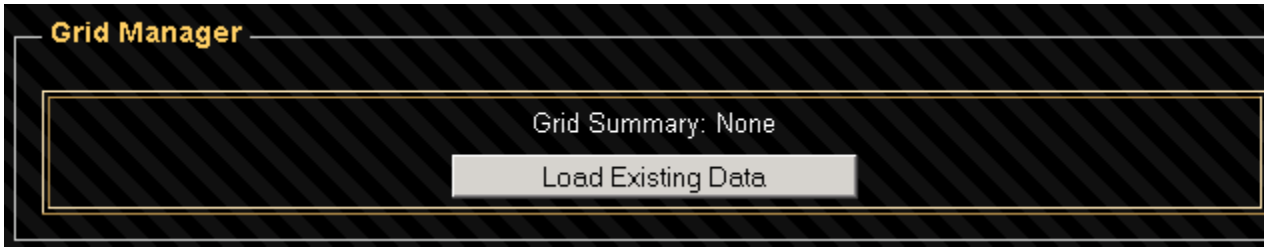


EMAIL VALIDATION BACKGROUND JOBS

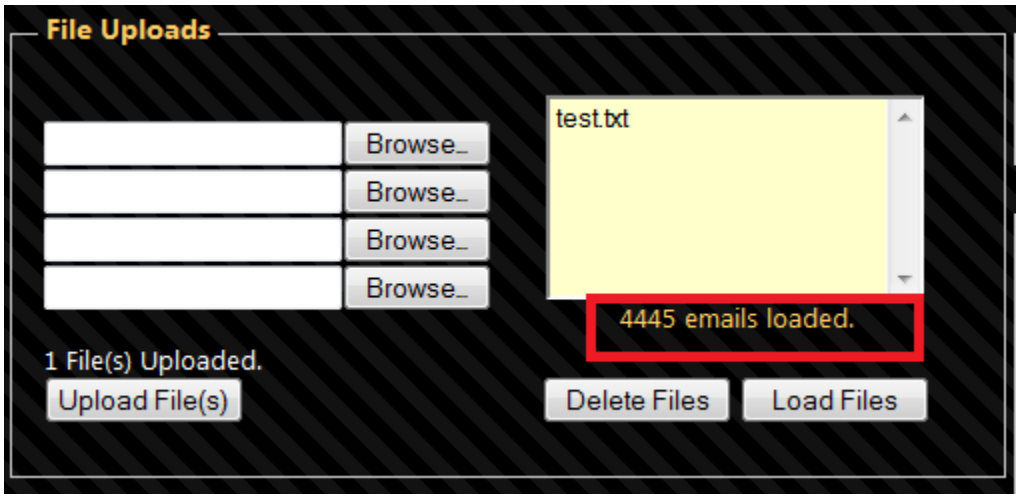
Swift Email Verifier supports email validations jobs as a background process in case the browser is closed or if the browser crashed while the validations are running and can also retrieve the last or ongoing verification job results that were performed. Should you close the browser or should your browser crash while the verifier job is running, you can retrieve the results of the validations by logging into the web verifier interface again and click on the "Load Existing Data "button. This will retrieve the results of the current active job.

Note that due to the nature of the session ID behavior in the application, you must close the full browser window before you will be able to access the application URL again. Otherwise, you will not be able to access the application if you closed only the application tab. If you have closed only the

application tab while other tabs are open in your browser, you may not be able to access the application URL.

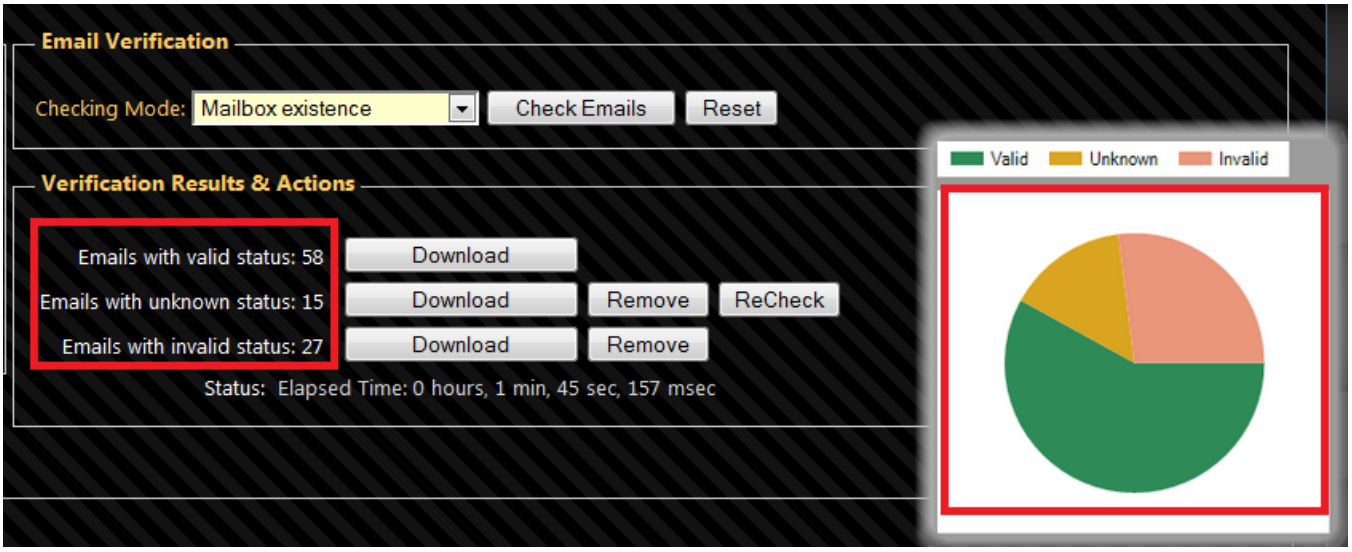


Clicking the button will populate the Grid with the current background validation jobs that has been completed while the browser was closed. To get the updated result, click on this button after some time interval until the total number of emails loaded for the verification job is equal to the total number of emails reported by the Grid system. You should compare the total number of emails in the Grid with the total number of emails loaded into the validation job in order to confirm if all the emails loaded have been successfully verified.



As the background job is running, the results and statistics pie chart figure is also updated each time the "Load Existing Data" button is clicked. The statistics are also updated automated when the job is running. This is illustrated in the screenshots below.

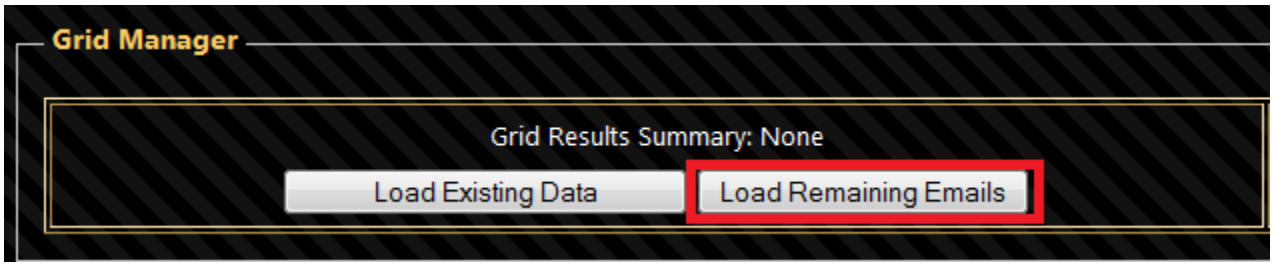
Note: Make sure you save the background job validation results and the Grid results excel file before loading a new mailing list as doing so would completely remove all the results of the background job.



Note: If you need to run a big list in the verifier and you do not want to keep your browser open while waiting for the progress bar to complete, you can close the browser while the job is running which will make the job run in background mode. Thereafter you can login again to the application to monitor the progress of the job by periodically clicking on the "Load Existing Data" button. This way, you can monitor the progress of the job without having to keep your browser open.

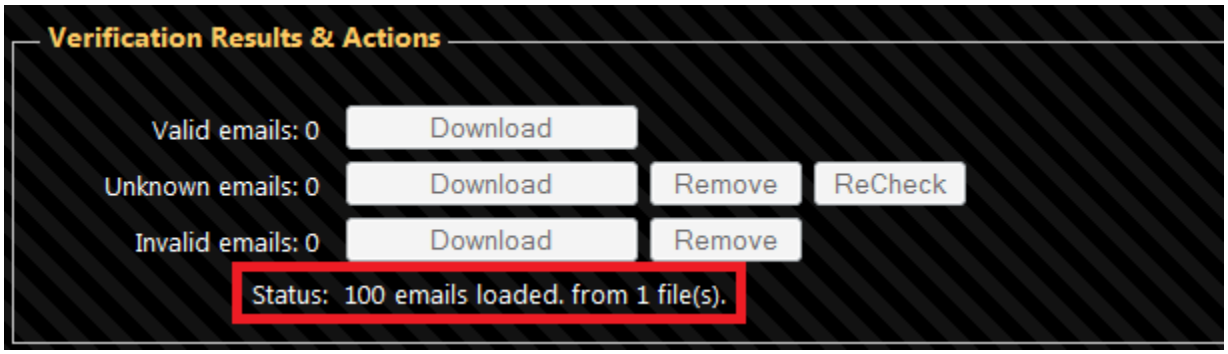
VALIDATING REMAINING EMAILS IN STOPPED JOB

Swift Email Verifier is able to load any remaining emails that could not be verified in an active running job due to mishaps such as server downtime or other issues that could cause the validation job to stop prematurely. If a validation job has stopped prematurely, you can use the “Load Remaining Emails” button to load the remaining emails that have not yet been verified in the stopped job. After loading the email lists, these remaining emails will be automatically loaded into the Grid so that a new verification can be performed using these emails as usual.

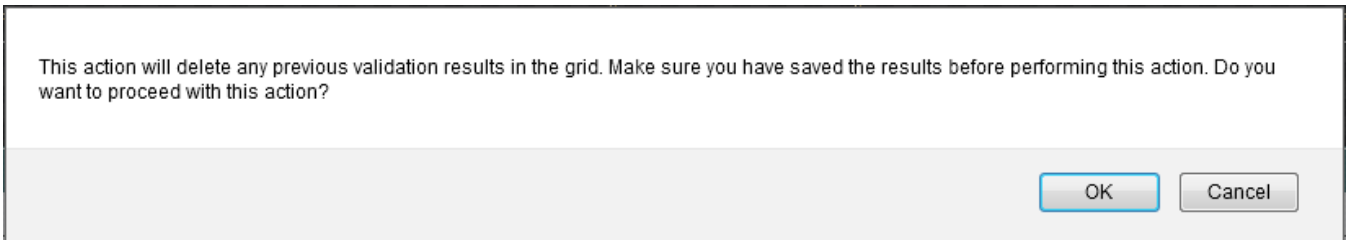


The total number of remaining emails that is loaded and populated in the grid will be displayed in the status notification of the application as illustrated in the screenshot below. Note that the number of

emails loaded will be the total number of emails loaded for the verification job minus the number of emails that were verified before the job stopped. However, note that this numbers may not add up if there are still some threads executing in the background even after the job has stopped. It usually takes some minutes for all threads to stop after a job dies.

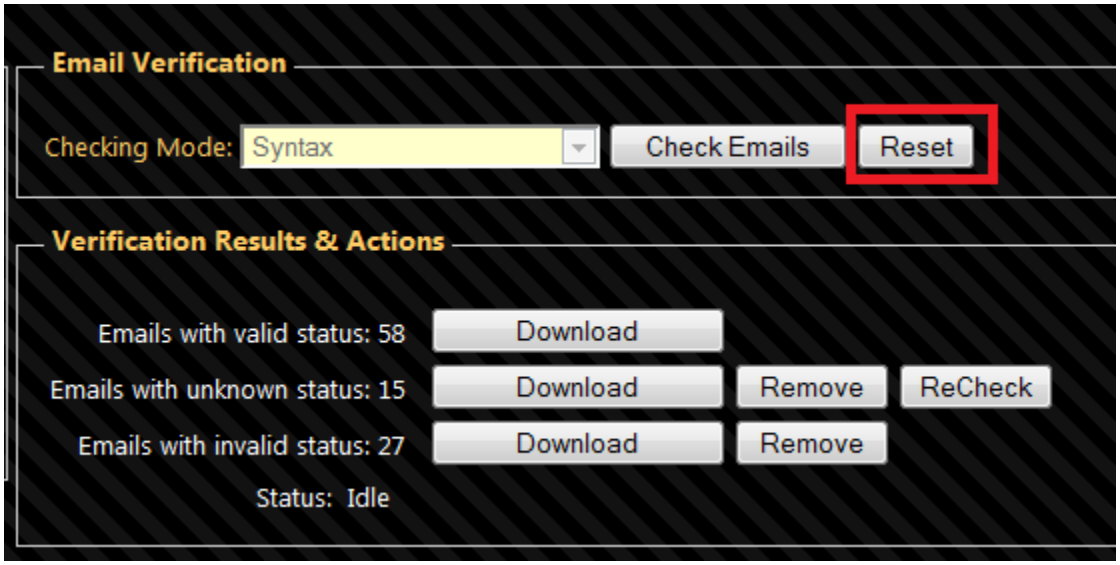


Please note that clicking the "Load Remaining Emails" button will delete any delete the already completed validation results in the system. Therefore, you must ensure that you have saved the results before performing this action.

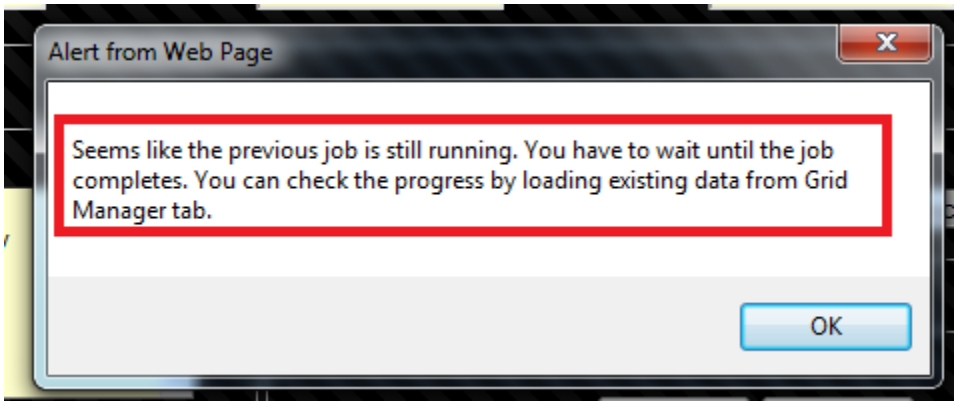

This action will delete any previous validation results in the grid. Make sure you have saved the results before performing this action. Do you want to proceed with this action?
OK
Cancel

RESETTING VALIDATION JOBS

If you wish to stop an ongoing or active validation job you can terminate it by closing the browser and resetting the validation jobs. Note that simply closing your browser will not terminate the active verification job which was running when the browser was closed. If the browser is closed, the verification job will continue to run in the background. Hence, you must reset the job by clicking on the "Reset" button in the Email Verification group menu. After clicking the "Reset" button, you must wait for a couple of minutes (3-5 minutes) in order for it to complete successfully because many threads will be executing together and all threads will be getting stop instruction when an async method is called by the thread.



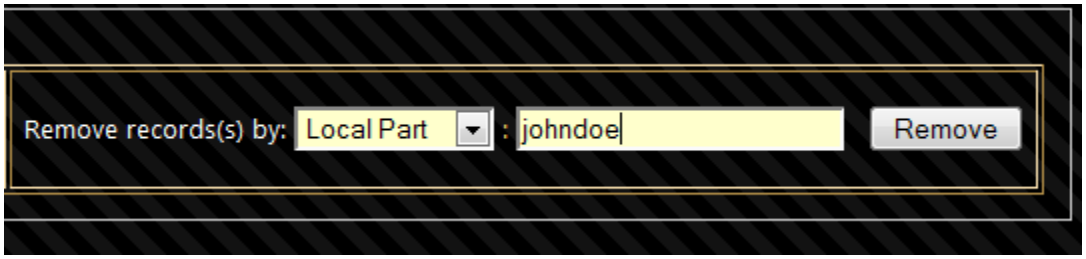
Be aware that once a verification process is already active and ongoing, it is not possible to start a new one. Any attempt to perform any tasks such as mailing list uploads or delete or new verifications will be denied. You will get the alert message shown below when the system detects such. If you wish to terminate the active job, click on OK and then proceed to click the Reset button. After this, you will be able to perform any other tasks.


Alert from Web Page
Seems like the previous job is still running. You have to wait until the job completes. You can check the progress by loading existing data from Grid Manager tab.
OK

REMOVING RECORDS FROM THE GRID

The desired email address records can be removed from the grid. The Email, Email Local Part, Domain and TLD records can be removed from the grid by typing the data and clicking on Delete as shown in the illustrative screenshots below. This feature is useful in situations where you want to delete one-way communications email addresses such as no-reply@domain.com, do-not-reply@domain.com, donotreply@domain.com, noreply@domain.com etc or if you wish to delete certain problematic email domains that are difficult or impossible to validate.

Removing records by Email address



Removing records by Email Local Part

Removing records by Email Domain

Removing records by Email domain Top Level Domain (TLD)

BOUNCE HANDLER AND MAILING LIST CLEANING

A unique feature of Swift Email Verifier is that in addition to the email verifier module, it also includes an automated bounced email processing module which takes care of those emails that cannot be

verified by simulating a message sending because the recipient email server requires that a REAL message is sent. Thus, it is impossible to verify whether the address is good or not. You won't know definitively until some bounce because these mail servers won't cooperate or cannot be checked without sending a real message to them. The bounce handling module can be used to process your bounced email messages and clean your mailing list

However, please be aware that some emails which return unknown results could be valid. Examples of such emails which are flagged unknown by the verifier and which may be valid are:

• Disposable Email Addresses from email address providers, like Mailinator, 10MinuteMail, GuerrillaMail,etc
• Catch-all email addresses
• Temporarily Unavailable emails (Graylisting)
• Soft bounces

Please note that in particular due to strict Yahoo anti-spam policies, deactivated or discontinued Yahoo emails may return as Valid emails in the verifier because Yahoo regards these deactivated or discontinued emails as valid although they are not active and cannot receive email. Hence when you attempt to send emails to such emails, it will bounce. This is why we strongly recommend the use of our bounce handler in the verifier.

Since no verifier service can offer 100% validation success, the bounce handler is used to compensate for it because it is impossible to verify all emails technically. So those emails that could not be verified and which are invalid would bounce. So by using the bounce handler, you can then extract these emails and delete them from your list so that you do not send emails to them anymore in subsequent campaigns. Then approximate 24-72 hrs, the bounce handler can be used to connect to the bounce-to email address which will enable it login to the email account, read all bounced emails and extract the emails and collect them in a text file. You can then download the file and subtract them from your master mailing list.

If your ESP do not offer you an option to specify your own bounce-to email address, we strongly advise that you do not send campaign to the unknown emails via your ESP because most ESPs have a very low tolerance for high bounces and if you exceed the bounce limit, your account may be suspended. So what we advise is that you purchase a bulk mailing program if you do not already have one and use free email SMTP servers specifically for handling your bounces. When choosing the email program, make sure that it can rotate between SMTP servers after a preset limit has reached . If you need such mailing software that offers this functionality, we do offer one. For details, please go to: www.smtpswitchmailer.com

We know that the main reason why email marketers use trusted third party ESPs is because they want high inbox. However, sending the emails initially using your own bulk mailing program and a private SMTP is the best option if you simply want to detect the email bounces first which could not verified with the verifier because the emails would still get delivered although a a majority may land in junk.

If you need help with installation of a private SMTP server on a centos server or VPS, we offer SMTP installation service for an affordable amount. For details, please go to:

http://bulkmailer.cc/smtp.htm

Note: our verifier has an easy way for you to filter out all yahoo emails verified as VALID and you can save these as a separate file and use your bulk mailing program to send your campaign to yahoo emails. Due to very strict Yahoo anti-spam policies, it is very risky to send emails to yahoo emails validated as VALID from any verifier.

Please note that email bounces can be problematic if not carefully handled. Continuous sending to invalid or non-existent email addresses leads to your IP address being blacklisted by your ISP and hurts your sender reputation. Sending email to invalid addresses negatively affects your sender reputation which is monitored by Yahoo, Gmail, AOL, Hotmail and other ISP's. The lower your reputation, the more your email gets delivered to junk since sender's IPs with low Sender Scores are rejected by most email ISPs. A Bounce Rate of 0.2-0.9 % typically has a Sender Score of 80-100% with a corresponding Inbox Delivery Rate of 90-99%.

Tip: We strongly recommend that you use the bounce handler to re-validate the “Unknown” email validation results which could not be verified due to one reason or the other. Simply send your email campaigns to the Unknown list and use the bounce handler to process and download the bounce email list. Then after getting the bounce list, subtract it from the unknown results list to obtain the clean list.

How Bounce Handler Works:

When you send your campaigns to a specific mailing list, invalid addresses will bounce back to you. Bounce message, also called a (failed) Delivery Status Notification (DSN) is an automated electronic email message from a mail system informing the sender about a delivery problem. The original message is said to have bounced. These bounced e-mails can be processed with the in-built bounce handler module in Swift Email Verifier to extract the bounce e-mail addresses (Bounce List). After you have the Bounce List, you can remove them from the mailing list that was used to send the campaigns.

Note that email bounces are either classified a soft or a hard bounce. Hard bounces are addresses denied for delivery due to invalid emails, blocked emails, emails reported for fraud/abuse or an unexpected error during sending. Soft bounces are recognized by the recipient's mail server but are returned to the sender because the mailbox is either full or temporarily unavailable. Swift Email Verifier does not make any distinction between these two categories of bounces. All bounces are processed. However, the bounce list can be run through the verifier module of the application at a later time to identify the soft bounces.

Note: Please note that for cost effectiveness reasons, it is strongly recommended to verify a mailing list once every 3-5 months and use bounce processing to wield out bounces from time to time which is a standard practice among all email marketers.

Your online verifier account be active for up to 6 months to allow you use the inbuilt automated bounce processing within 6 months after validating your emails and sending your campaigns to the emails. Although your account will have a fixed validation limit quota that you have purchased, this limit does not expire and you can use it anytime and whenever you want. The use of the bounce handler does not count towards your validation credits.

The bounce handling takes place in the following sequence:

- **User Specifies Bounce Email Address and Connection Details:** Bounced emails are sent to a dedicated central bounce email address such as bounce@domain.com which has to be specified by the user. We highly recommend the use of a dedicated e-mail address for this purpose. Please note that depending on your email settings, a dedicated bounce email address may not exist.

However, because most email servers do recognize the “From” email address (otherwise known as the Sender envelop address) automatically as the bounce email address, you can specify the “From” address as the bounce email address in our bounce handling module. With our bounce handler module, you don’t need to worry about having a dedicated bounce email address. You can also use your “From” address because the bounce handler uses powerful algorithm to analyze your inbox messages and detects the bounced messages from other messages.

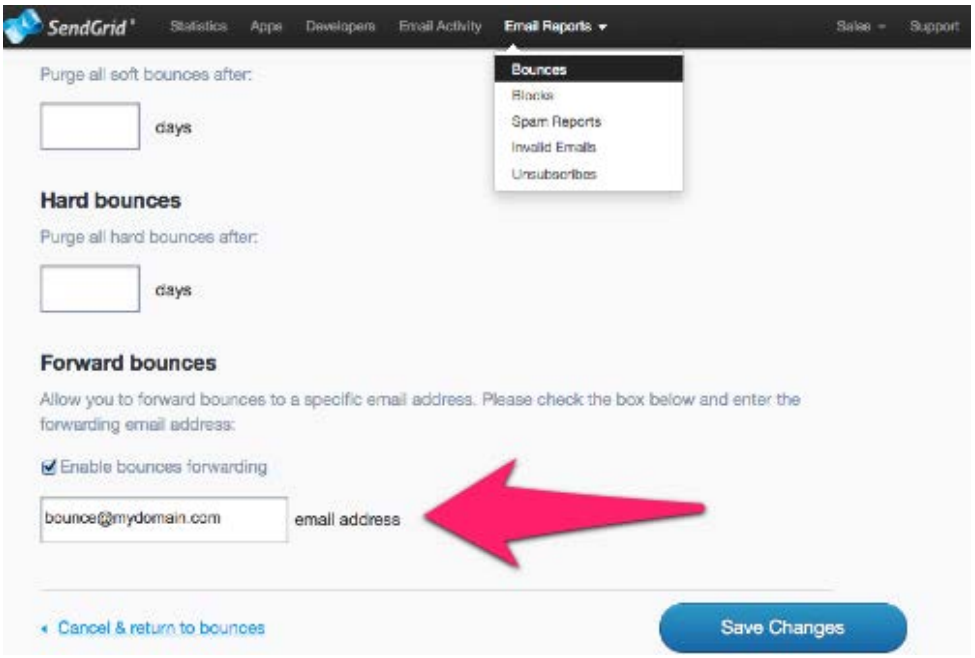
Some ESP like SendGrid or Elastic Email do allow you to specify your own bounce email address. If you use any of these, you can configure them to forward your bounces to **a single dedicated Gmail bounce address**, like bounce@gmail.com. Then on the verifier bounce handler, you can then enter the Gmail bounce email connection settings and have the bounce handler process the bounces.

SendGrid & Elastic Email allows users to specify their own bounce address so they can handle the bounces themselves.

Simply ask SendGrid or Elastic Email to forward these bounces to your own bounce address so that you can use this bounce email address in the verifier to process your bounces.

Configuring bounce email in SendGrid:

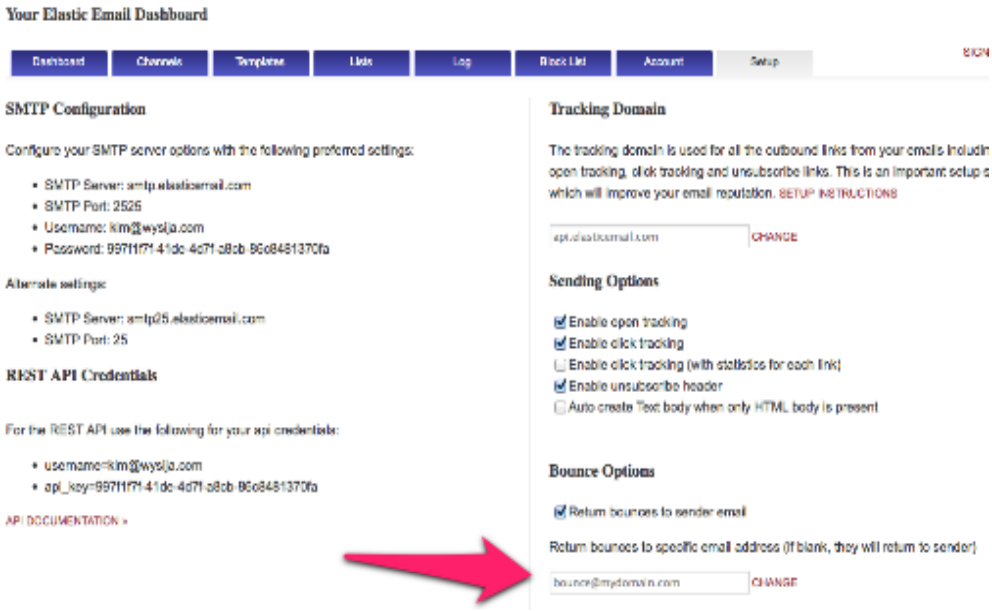
In SendGrid, go to Email Report > Bounces. Click on the “Settings” link to be directed to the bounce options page.



Configuring bounce email in SendGrid:

==========

In Elastic Email, find the option in the Setup tab:



Sending and/or bounce handling with Gmail

However, if you decide to use a Gmail account to send and process your bounces, the following rules must be strictly followed:

1. it has to be on the **same domain** as the sender's address. If you're sending from *info@**gmail.com***, then your bounce could be *bounce@**gmail.com***
2. the bounce address is dedicated solely to bounces, nothing else

3. If you send with Gmail, you have to handle the bounce with the same Gmail account. Otherwise, spam filters will be suspicious.

We strongly recommend that you create a dedicated Gmail account not used for any other purpose for processing your bounces.

In order to connect to the mail server, the IMAP or POP3 settings have to be provided also. The following table lists IMAP and POP3 settings for popular email ISPs:

Email ISP	IMAP Server Name	POP3 Server Name	IMAP SSL Port	POP3 SSL Port
AOL	imap.aol.com	pop.aol.com	995	993
Hotmail/Outlook	Not Supported	pop3.live.com	995	NA
Yahoo	imap.mail.yahoo.com	pop.mail.yahoo.com	995	993
Yahoo Mail Plus	plus.imap.mail.yahoo.com	plus.pop.mail.yahoo.com	995	993
Yahoo UK	imap.mail.yahoo.co.uk	pop.mail.yahoo.co.uk	995	993
Yahoo Germany	imap.mail.yahoo.de	pop.mail.yahoo.de	995	993
Yahoo AU/NZ	imap.mail.yahoo.com.au	pop.mail.yahoo.com.au	995	993
AT&T	imap.att.yahoo.com	pop.att.yahoo.com	995	993
Googlemail/Gmail	imap.gmail.com	pop.gmail.com	995	993

- **Bounce Handler Connects to the IMAP or POP3 Mail Server:** In order to use our bounce handler, you must provide the bounce-to email IMAP or POP3 connections details. Using the provided IMAP/POP3 settings and login credentials, our bounce handler will connect to the mail server and scan all messages in the inbox of the bounce email address provided. It then uses Multipart/Report mime parts (defined in RFC 6522) to recognize bounce messages, as well as other heuristics (X-Failed-Recipients header, subject and body scanning). Once the bounced messages are detected, the email addresses are extracted and the bounced messages are marked as "READ". Optionally, when requested by the user, the bounce handler can delete all the bounced messages from the email server. The bounce list is then made available for the user for download or for cleaning the mailing list from which the campaign(s) was sent.

- **Bounce Handler Cleans the Mailing List Using the Bounce list:** After generating the bounce list, the bounce handler then subtracts this list from the original mailing list which was used in sending the campaigns. The user has to upload this mailing list.

HOW TO USE BOUNCE HANDLER AND MAILING LIST SUBTRACTION MODULE

The following steps show how to use the bounce handler and mailing list subtraction module of Swift Email Verifier:

Step 1: Go to the "Bounce Handler and Mailing List Subtraction" group in the program interface and enter your incoming Mail Connection Settings. Both IMAP and POP3 incoming mail protocols are supported. The following fields are required:

- **Bounce-To Email:** This field indicates the email address where your bounces are received. This field also represents in most cases the Username to connect to this e-mail address. We highly

recommend you to handle your bounce messages on a dedicated mailbox. That way, you won't receive the replies from your subscribers on this same mailbox and you will safely allow the bounce handler module to delete messages from your bounce mailbox.

- **Password:** Password used to connect to your bounce-to e-mail account.
- **IMAP/POP3 Server:** This is the IMAP or POP3 server protocol name. Please select the appropriate protocol from the drop-down box.

  Tip: If your mail server supports both POP3 and IMAP protocols, it's recommended that you use the IMAP protocol as the speed of processing bounced emails from an IMAP account is several times higher than from a POP3 account depending on multiple network factors such as internet speed, size of emails and email server connection.
- **Port:** This is port required for the connection. Default is 993 for IMAP and 995 for POP3 (using a secured SSL connection).
- **Use SSL:** Tick this if using the secured connection port
- **Delete Bounces:** Tick this if you want the bounce handler to automatically delete all bounced messages from the email server after they are processed. This is strongly recommended in order to increase the speed of the processing.

Note: If you use Gmail IMAP server and want the bounce handler to delete the bounced messages, make sure you enable IMAP and setup the IMAP settings in Gmail as shown in the screenshot below. Otherwise, the program won't be able to delete bounced messages from the server.

IMAP Access:
(access
from other clients using IMAP)
Learn more
Status: IMAP is enabled
Enable IMAP
Disable IMAP
When I mark a message in IMAP as deleted:
Auto-Expunge on - Immediately update the server. (default)
Auto-Expunge off - Wait for the client to update the server.
When a message is marked as deleted and expunged from the last visible IMAP folder:
Archive the message (default)
Move the message to the Trash
Immediately delete the message forever

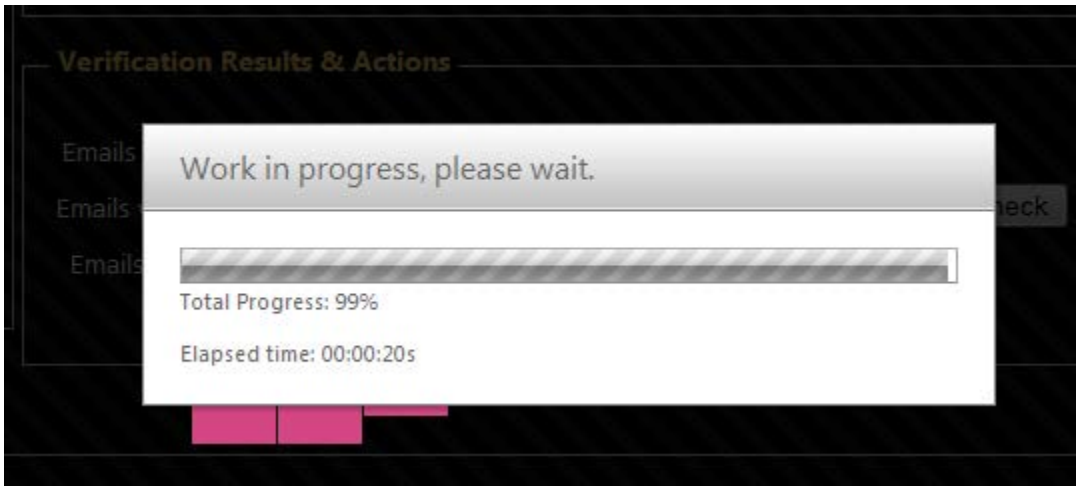
To enable IMAP in Gmail:

1. Sign in to Gmail.
2. Click the **gear icon** in the upper-right and select **Mail settings.**
3. Click **Forwarding and POP/IMAP**.
4. Select **Enable IMAP**.
5. Now you are able to connect to your Gmail account with our Bounce Handler

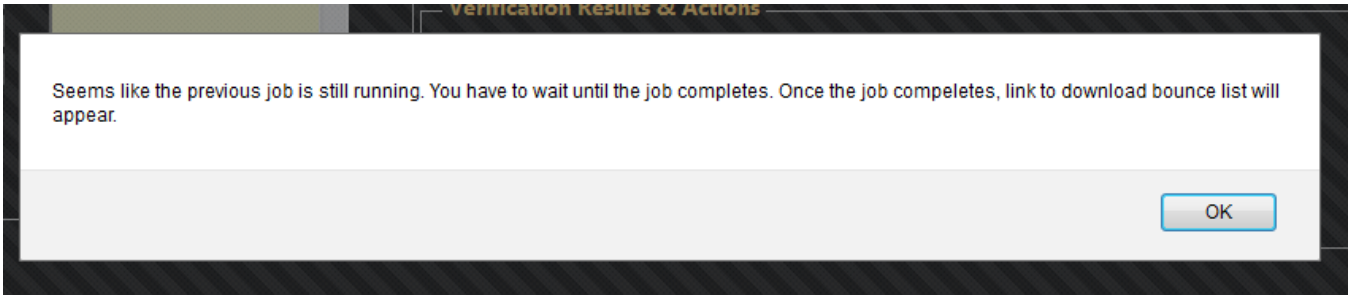
Remember that Gmail only allows secure SSL connections so you need to use SSL port 993.

Note: If you do not know your email server settings, please inquire from your ISP or email provider.

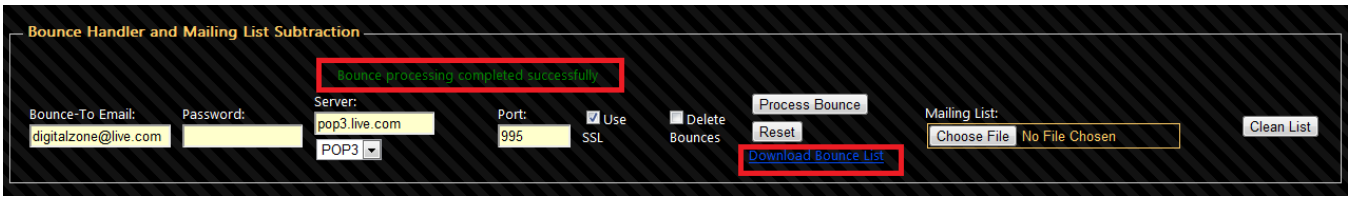
Step 2: Click on the "Process Bounces" button to execute the bounce processing. Please note that this action can take a while to complete depending on your mail server connection and volume of bounced emails. A progress bar indicating the progress of the bounce processing will appear. Once the process is completed, the system will alert you and you will see the "Bounced Processing Completed Successfully" message. In addition, the generated Bounce List will be made available for download.



The processing also supports background mode in the event of browser closed or if your browser or system crashes so that the processing can continue in the server. Once you login again to the application interface and the processing has completed, the download link to download the bounce list will automatically appear. Please note that while a bounce processing job is active, a new bounce processing job cannot be started. You must wait for the ongoing process to complete before attempting to start a new one. If you wish to stop the processing, you can do so by clicking the "Reset" button. Doing so will terminate the process.

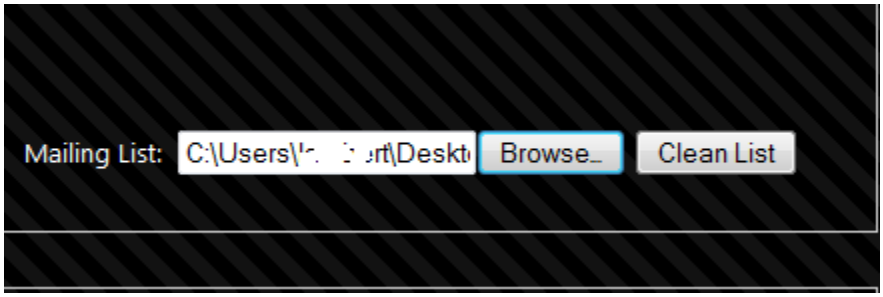

Verification Results & Actions
Seems like the previous job is still running. You have to wait until the job completes. Once the job compeletes, link to download bounce list will appear.
OK

Step 3: When the bounce processing is complete, download the bounce list and save it on your PC. It is advisable to run this list through the email verifier module in order to detect possible soft bounces at a later time.



Step 4: Upload the mailing list which was used to process the bounces. If you have used multiple mailing lists for your campaigns, make sure you combine all the lists in a single mailing list before uploading it.

Step 5: Click on the "Clean List" button to subtract the bounce list from the mailing list you have uploaded. Doing so will automatically remove all bounced email addresses from the mailing list leaving only the clean ones.



Step 6: Download your cleaned list

DISCONNECTING FROM SWIFT EMAIL VERIFIER

After validating your emails and you wish to end your session, you can easily disconnect from the verifier by clicking on the “Disconnect” link at the upper right hand side of the verifier interface. Note that if you are logged into the Swift Email Verifier and you session becomes idle for more than 30 minutes; you will be automatically re-directed to the verifier logon screen. Simply re-login to continue to access the application.

FREQUENTLY ENCOUNTERED ISSUES AND TROUBLESHOOTER

Problem 1: Active validation job appears stuck or dead and not progressing

How to fix: Due to mishaps such as server downtime or other issues, it is possible for your active validation job to stop prematurely. To fix this, you must kill the job by clicking on the "Reset" button and wait for about 3-5 minutes for this action to propagate in the server. Then click on the "Load Existing Data" button to retrieve the already completed job results and make sure you save the results to your computer. Then finally reload the remaining emails that has not been verified by clicking on the "Load Remaining Emails" button. After you load the list, run the verification on these remaining emails which were not verified before the job stopped.

Important Information: Please note that clicking the “Load Remaining Emails” button will delete the current or last completed validation job results already completed in the system. Therefore, you must ensure that you have saved the results before performing this action.

Problem 2: Unable to login to the verifier interface

How to fix: First, make sure you are using the correct credentials. In addition, please note that when you have an active batch verification job running and you close the browser, you will be unable to access the page unless you close the whole browser and open the URL again due to session state. To address this, if you are running an active job in your account and you close the browser and you wish to access the application again, you can use the alternate URL. Both URLs can be alternated in the event of connection issues. Regardless of the URL used, your verification results data can be retrieved from any of the instances.

Problem 3: Getting Runtime errors due to active session timeout

How to fix: If you are logged into the verifier and your active session becomes idle for some minutes, you may experience timeout errors or Runtime errors when you try to perform any action on the verifier. To fix this, simply logout from the verifier by clicking on the “Disconnect” link at the upper right hand side in the verifier interface and login again.

SWIFT EMAIL VERIFIER

FREQUENTLY ASKED QUESTIONS

Question 1: How does your email validation process work?

Answer: Our email validation system can be used to validate emails effectively using the following order of validation processing:

- **Syntax Check:** This checks the email addresses and ensures that they conforms to IETF standards using a complete syntactical email validation engine
- **Mail Server Existence Check:** This checks the availability of the email address domain using DNS MX records
- **Mail Existence Check:** This checks if the email address really exists and can receive email via SMTP connections and sending email emulation techniques.
- **Catch-All Domain Email Check:** This checks if the email domain will receive all of the email messages addressed to that domain, even if their addresses do not exist in the mail server
- **Disposable Email Address Check:** This checks if the email is provided by a known Disposable Email Address (DEA) provider such as Mailinator, 10MinuteMail, GuerrillaMail and about 2000 more

Question 2: How is your email validations performed? Does it send out any email?

Answer: The email validation system employs DNS and SMTP protocol functionalities to perform email address validations and absolutely avoids sending any email message to external mail servers.

The Email validation process is done using 3 progressive levels automatically as follows:

- **Syntax** : This checks the email addresses and ensures that they conforms to IETF standards using a complete syntactical email validation engine
- **Email Server Existence** : This level checks the availability of the email address domain using DNS MX records
- **Mailbox Existence** : This is a deep level verification which attempts to check if the email address really exists and goes a step further to check if the email domain is a Catch-all domain (a domain that will receive all of the email messages addressed to that domain, even if their addresses do not exist in the mail server). The Mailbox verification establishes SMTP dialogs with external SMTP servers and this level usually requires longer time depending on multiple network factors.

Question 3: Is it possible to verify all emails with your email validation service? How does the system handle Unknown emails?

Answer: It is not possible to validate all emails due to multiple factors beyond our control. The Unknown results are those emails which could not be verified due to one reason or the other. These unknown results in most cases results from Greylisting which is technology that reduces spam by rejecting initial email delivery attempts. The Greylisting works by returning a "Temporarily Unavailable" message to the sending mail server the first (and only the first) time a message is received from a given sender. Hence, it makes sense to retry these validations again after some time has elapsed.

In addition, unknown results can also result from the inability to verify the emails by simulating a message sending to the recipient email server because the recipient email server requires that a REAL message is sent. Thus, it is impossible to verify whether the address is good or not. You won't know definitively until the message bounce because these mail servers won't cooperate or cannot be checked without sending a real message to them. To accommodate for this, the verifier includes an in-built bounce handling module that can be used to process the bounced emails to the unknown results list. For details, please click here.

Question 4: Can I achieve low bounce rates with the email validation service?

Answer: One of the main reasons why you must validate your emails regularly is to ensure that you avoid high bounce rates when you send your campaign to your lists. When you send emails to invalid emails, the message will bounce. A bounced message is one that has been rejected by the recipient's email server. If your emails get bounce rates of over 10-15%, your email marketing service provider may likely disable your account until you can determine the cause of the bounces. This is because high bounce rates can get your email marketing service provider IPs blacklisted and will also negatively affect your sender reputation which will result to poor inbox deliverability. There are two types of bounces as follows:

- Hard bounces: These are bounces caused as a results of permanent failure during delivery (typically 5.x.x / Mailbox does not exist at the domain)

  Please see : http://www.basics.net/index.php/2011/07/27/e-mail-smtp-error-codes/

- Soft Bounces: These are bounces caused by temporarily failure such as Mailbox full errors ((beginning with a 4.x.x code as seen in above link)

With our email validation system, you will be able to verify your emails and detect a good number of emails that would have bounced (hard bounces) and these will be marked "Invalid". Hence, you will be able to stay within the acceptable bounce rate limits typically permitted by email service providers. Emails with soft bounces will be marked "Unknown" and has to be revalidated. However, to identify

emails with soft bounces which could turn out to become valid later, it is advisable to re-validate the unknown emails again after some days (1-3 days).

Question 5: Why are some invalid emails sometimes marked as Valid?

Answer: First, it is important to understand that our email validation technology uses the SMTP connection method to check whether a specific email address is valid or not by simulating email sending. However, due to certain multiple factors such as anti email harvesting technology, it is not possible to verify all emails with 100% success rate. This is because some mail servers such as public mail servers like Yahoo, AOL, etc have some measures in place which makes it impossible to accurately determine whether the email is valid or invalid because the mail servers will not cooperate and as a result the email address will be marked as valid when validated.

For example, Yahoo will always mark disabled or discontinued emails as Valid when verified. However, when you try to send to such disabled or discontinued emails, it will return this error message:

Remote server replied: 554 delivery error. Sorry your message to <email_address> cannot be delivered. This account has been disabled or discontinued.

For such mail servers, the only means to conclusively know if the email is valid or not is when the email bounce. Hence, it is recommended to use the bounce handler in the verifier to process the bounces for such non cooperating mail servers in order to obtain the invalid emails. For details on how to use the bounce processing feature of the verifier, please click here.

GETTING SUPPORT

If you have any questions or encounter any issues while running the application, you can reach our support center by visiting http://www.webemailverifier.com/supportsuite/ Always ensure that you provide your member username when creating trouble tickets in order to assist us to resolving your issues as quickly as possible.